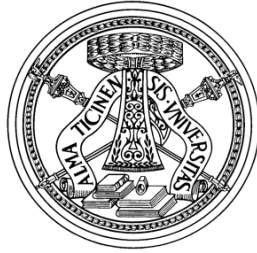


UNIVERSITÀ DEGLI STUDI DI PAVIA



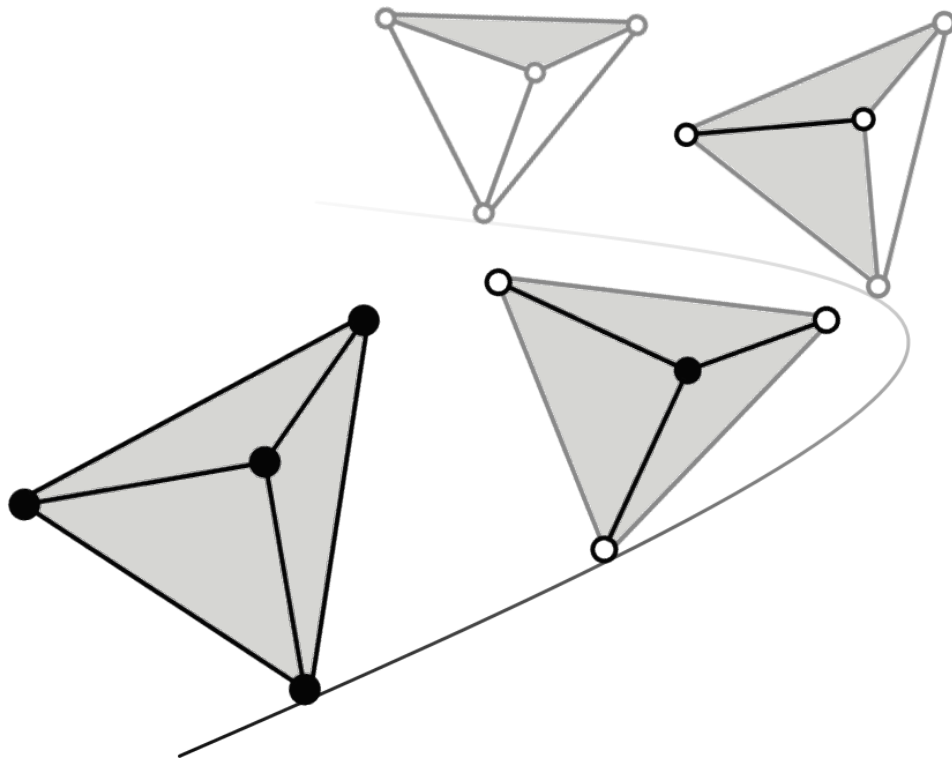
DOTTORATO DI RICERCA IN FISICA - XXVI CICLO

---

# Entanglement in Quantum Algorithms and Quantum Channel Detection

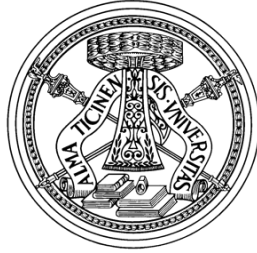
Matteo Rossi

---



TESI PER IL CONSEGUIMENTO DEL TITOLO

UNIVERSITÀ DEGLI STUDI DI PAVIA



DOTTORATO DI RICERCA IN FISICA - XXVI CICLO

---

# Entanglement in Quantum Algorithms and Quantum Channel Detection

Matteo Rossi

---

Adviser:

Prof. Chiara Macchiavello

Referees:

Prof. Vittorio Giovannetti

Prof. Dr. Otfried Gühne

SUBMITTED TO THE GRADUATE SCHOOL IN PHYSICS  
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF  
DOTTORE DI RICERCA IN FISICA  
DOCTOR OF PHILOSOPHY IN PHYSICS  
AT THE  
UNIVERSITY OF PAVIA

COVER: Depiction of hypergraphs associated to the four-qubit initial Grover states with two solutions for several values of the Hamming distance. Each empty vertex represents a qubit. Full dark dots, dark lines and grey faces represent hyperedges of order 1, 2 and 3, respectively.

**Entanglement in Quantum Algorithms  
and Quantum Channel Detection**

Matteo Rossi

PhD thesis — University of Pavia  
Printed in Pavia (Italy)  
October, 2013

ISBN 978-88-95767-65-9

# Acknowledgements

A special thanks goes to Chiara that supervised my work and continuously supported me along my PhD. Another special thanks goes to Dagmar and her group in Düsseldorf, as I really enjoyed my experience there. Huge thanks to the Quit group, especially to the youngest part, with which I shared more food and drinks than physics. I am really in debt with Marcus Huber that gave me the change to visit many places while doing exciting physics. At last, I am grateful to Otfried Gühne and Vittorio Giovannetti for refereeing my thesis and giving me several fruitful feedbacks.



# Contents

<b>Introduction</b>	<b>1</b>
<b>1 Quantum Hypergraph States</b>	<b>5</b>
1.1 Real equally weighted states . . . . .	5
1.2 Standard graph states . . . . .	7
1.3 $k$ -uniform hypergraph states . . . . .	9
1.4 Hypergraph states . . . . .	12
1.5 Equivalence between hypergraph and REW states . . . . .	14
1.6 Comments and future work . . . . .	16
<b>2 Entanglement in Grover's Algorithm</b>	<b>17</b>
2.1 Some remarks about Grover's algorithm . . . . .	17
2.2 Entanglement content of initial states in Grover's algorithm . .	18
2.2.1 Single solution . . . . .	19
2.2.2 Two solutions . . . . .	20
2.2.3 Connection to hypergraph states . . . . .	22
2.3 Entanglement dynamics in Grover's algorithm . . . . .	23
2.3.1 Single solution . . . . .	24
2.3.2 Two solutions . . . . .	26
2.4 Entanglement dynamics in the fixed-point $\pi/3$ quantum search algorithm . . . . .	28
2.5 Classical simulatability of Grover's algorithm . . . . .	29
2.6 Conclusions and comments . . . . .	31
<b>3 Quantum Channel Detection</b>	<b>33</b>
3.1 Main idea and mathematical tools . . . . .	33
3.1.1 Entanglement detection . . . . .	34
3.1.2 Quantum channels and the Choi-Jamiołkowski isomor- phism . . . . .	35
3.2 Entanglement breaking channels . . . . .	36
3.3 Separable random unitaries . . . . .	38
3.4 Separable maps . . . . .	42

## CONTENTS

---

3.5	PPT channels . . . . .	45
3.6	Completely co-positive channels . . . . .	47
3.7	Bi-entangling operations . . . . .	49
3.8	Summary and further developments . . . . .	51
<b>4</b>	<b>Map Detection: Noise Robustness and Experimental Realization</b>	<b>53</b>
4.1	Detecting the CNOT and CZ gates . . . . .	53
4.2	Noise robustness . . . . .	55
4.2.1	Depolarising noise . . . . .	56
4.2.2	Dephasing noise . . . . .	58
4.2.3	Bit flip noise . . . . .	60
4.2.4	Amplitude damping noise . . . . .	62
4.3	Experimental detection of quantum channels . . . . .	64
4.3.1	Single-qubit EB channels . . . . .	64
4.3.2	Two-qubit separable maps . . . . .	67
4.4	Conclusions and further perspectives . . . . .	70
<b>5</b>	<b>Quantum Cloning by Cellular Automata</b>	<b>73</b>
5.1	Two fundamental preliminaries . . . . .	73
5.1.1	Phase-covariant cloning . . . . .	74
5.1.2	Quantum cellular automata . . . . .	74
5.2	Phase-covariant cloning by QCAs . . . . .	76
5.2.1	Performances in the rest frame . . . . .	78
5.2.2	Performances exploiting different foliations . . . . .	79
5.3	Summary of results . . . . .	81
	<b>Conclusions</b>	<b>83</b>
<b>A</b>	<b>Appendix</b>	<b>85</b>
A.1	Group structure of the generalized stabilizer operators . . . . .	85
A.2	Equivalence of the circuital definition and the stabilizers description . . . . .	86
A.3	Inequivalence of $k$ -uniform hypergraphs under the local Pauli group . . . . .	87
<b>B</b>	<b>Appendix</b>	<b>91</b>
B.1	Asymptotic limit of the GME $E_n$ . . . . .	91
B.2	Calculation of the GME $E_2$ . . . . .	92
<b>C</b>	<b>Appendix</b>	<b>95</b>
C.1	Purity of the Choi state $C_{\mathcal{M}}$ . . . . .	95
C.2	Schmidt decomposition of $Z_3$ and calculation of $\alpha_{SRU}$ . . . . .	96

<b>D Appendix</b>	<b>99</b>
D.1 QCD experimental set-up . . . . .	99
D.2 Two-qubit CNOT gate: noise model . . . . .	100
<b>Bibliography</b>	<b>103</b>
<b>List of Publications</b>	<b>109</b>





# Introduction

The arguments discussed in this work can be roughly divided in two main topics: on the one hand we study the entanglement contents of the states employed in well-known quantum algorithms, while on the other hand we adapt some techniques suitable for entanglement witnessing in order to detect convex sets of quantum channels. Eventually a side result concerning quantum cloning via cellular automata is presented.

**Quantum computing and entanglement:** Quantum computation is one of the most prominent branch of quantum information science [1]. Despite there exist several examples of quantum algorithms that outperform classical computers, such as Shor's [2], Grover's [3], Deutsch-Jozsa's [4, 5] and Simon's [6] algorithms, the reason for such a quantum speed-up is not fully understood yet. One of the major candidates as fundamental resource is surely quantum entanglement. However, even though entanglement has been shown to be sometimes necessary in order to achieve an exponential speed-up [7, 8, 9], other results point in a completely opposite direction [10, 11, 12, 13]. Hence, the role entanglement plays with regards to quantum computing is nowadays still a heavily debated open question [14, 15].

The first part of this work is intended to shed new light on the role of entanglement in quantum computation by both developing mathematical tools in order to study specific states that appear in well-known quantum algorithms [16], and systematically studying the entanglement content of states employed in Grover's algorithm [17, 18]. On the one hand, the mathematical tools we develop are essentially related to graph theory, and are suitable to link real equally weighted pure states (i.e. superposition of all basis states with real amplitudes and equal probabilities) with hypergraph states. This ideal bridge allows us to study more easily states that very often appear in significant quantum protocols, giving a pictorial view of these in terms of mathematical hypergraphs. The entanglement properties of either a single state or an interesting class of quantum states are then pointed out and simplified drastically. On the other hand, a deep study of the entanglement content of states employed by Grover's algorithm provides us the entire dynamics of both bi-

partite and multipartite entanglement along the whole procedure. In addition, besides multipartite entanglement is shown to be always present along the Grover computation, a very peculiar and unexpected scale invariance property of entanglement emerges. Such a scale invariance property makes the study of Grover's algorithm closer to many-body systems and phase transitions, as they often show scale invariance properties too.

**Quantum channel detection:** Quantum channels represent the most general process a quantum system can undergo [1]. They are in addition a very convenient method to study several quantum information tasks that require a discrete-time evolution [1, 19], as e.g. quantum computation. From an experimental point of view, the characterization of a quantum channel is known to be highly resource-demanding, as it usually requires a very large number of measurement settings. It is then of great interest to develop techniques able to point out properties of interest of the channel, by avoiding full quantum process tomography. Furthermore, in many realistic situations one is mainly interested in a specific property of the channel, as e.g. whether it has some entangling power, rather than the full form of it.

Inspired by the recent field of entanglement witnessing [20, 21], in the second part of this work we develop a quantum channel detection method that works when some a priori information about the form of the channel is available [22, 23]. As the entanglement detection is an efficient way to prove that the state of interest is eventually entangled, the quantum channel detection method turns out to be a suitable technique to rule out meaningful subsets of quantum channels such as, e.g., entanglement breaking [24], separable [25] and positive partial transpose [26, 27] channels. The robustness of the method against noise is then extensively studied for several noise models such as depolarizing, dephasing, bit flip and amplitude damping [28]. Eventually an experimental implementation of the channel detection method is proposed and achieved for either entanglement breaking channels of the depolarizing form and the CNOT gate [29], a fundamental resource needed for universal quantum computing.

**Quantum cloning via cellular automata:** As a side result, we present also an application of the growing field of quantum cellular automata in order to perform one of the most important quantum information protocols, i.e. quantum cloning [30]. Even though the achieved result is not directly related to the two main arguments from which this work takes roots, it has to be regarded with particular interest. Indeed it fuses together the well-established task of quantum cloning [31] with the raising field of quantum cellular automata [32, 33], showing how an old-fashion concept still provides new insights if studied under a different perspective.

This work is organized in five chapters. The first two are devoted to studying the relationship that elapses between entanglement and quantum computa-

tional speed-up, by studying the class of states employed in many quantum algorithms, and in particular in Grover's. In the second two, the method of quantum channel detection is introduced and discussed in details both theoretically and experimentally. Quantum cloning via quantum cellular automata is presented in the last chapter, which constitutes a result on its own. Every chapter starts with a brief introduction, intended to recall the reader the context in which the argument is developed, and concludes with a few paragraphs summarizing the achieved results and discussing further possible developments.



# Chapter 1

## Quantum Hypergraph States

Quantum algorithms constitute one of the main applications of modern quantum information theory, and offer computational speed-up, that provably no classical system could ever exhibit [1]. Many quantum protocols, as e.g. quantum algorithms that admit an oracle description, such as Deutsch-Jozsa's and Grover's algorithms, usually employ real equally weighted (REW) pure states. Thus, this family of states plays a central role in several quantum tasks and might be the key to a deeper understanding of the role of entanglement in quantum speed-up.

We present here a way to fruitfully study such states. The method is based on a correspondence with mathematical objects called hypergraphs [16]. Quantum hypergraph states are then a straightforward generalization of very well-known graph states. However, besides being very close in spirit to these latter states, hypergraph states show a much richer entanglement structure. This feature basically allows us to exploit them to better understand and quantify the entanglement content of states employed in quantum algorithms.

The sketch of the chapter is roughly the following. We firstly show that hypergraph states indeed cover all possible REW states, and that they have an illustrative graph representation. Then we find that they are stabilized by generalizations of the stabilizers of graph states, and that they constitute a set of different entanglement classes under local Pauli operations. We finally discuss possible ways to extend our work, especially with regard to measurement-based quantum computing and entanglement witnessing.

### 1.1 Real equally weighted states

The  $n$ -qubit register employed in the Deutsch-Jozsa [4] and Grover [3] algorithms is initially prepared in the pure fully separable state

$$|\psi_0\rangle \equiv |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle, \quad (1.1)$$

## 1. Quantum Hypergraph States

---

which corresponds to the equally weighted superposition of all possible  $2^n$  states  $|x\rangle$  of the computational basis. The next step in both algorithms consists in applying a unitary transformation  $U_f$  that leads to the following state of the  $n$ -qubit register

$$|f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle, \quad (1.2)$$

where  $f(x)$  is the  $\{0, 1\}^n \rightarrow \{0, 1\}$  Boolean function that need to be evaluated in the considered algorithm. Notice that, since  $(-1)^{f(x)} = \pm 1$ , the state  $|f\rangle$  is uniquely defined by the function  $f$  via the signs (either plus or minus) in front of each component of the computational basis. For this reason the above states are named REW states, and the set is denoted by  $G_{\pm}$ . A more general class of equally weighted states, with generic phase factors in front of each computational basis state, and an explicit method to generate them was analysed in [34].

Due to their simple expression, we can count the number of REW states. If we fix the first state  $|00\dots 0\rangle$  to have always a positive phase (this essentially corresponds to disregarding a meaningless global minus sign), it turns out that they are  $2^{2^n-1}$ . Given a function  $f$ , we are essentially interested in finding out some properties of the corresponding state  $|f\rangle$ , such as the entanglement content. It is clear that these properties only depend on where the signs are placed. The same analysis can obviously be applied to families of states  $|f\rangle$ , where for instance the function  $f$  is taken to have a given property, as e.g.  $f$  constant or balanced as in the Deutsch-Jozsa algorithm.

In order to study this class of states, we can think to relate them to graph states. In the following we will nevertheless become soon aware that the class of graph states is not rich enough to account for all REW states. Due to that, we then focus on a wider class of states, i.e. hypergraph states, which can be seen as a generalization of graph states. We eventually find out that hypergraph states provide us a nice and useful tool to study and classify all REW states.

Regarding the notation, we very often use controlled  $Z$  gates acting on an arbitrary number of qubits. Given a system composed of  $n$  qubits, we denote by  $C^k Z_{i_1 i_2 \dots i_k}$  the general controlled  $Z$  gate acting on the  $k$  qubits labelled by  $i_1 i_2 \dots i_k$ . Notice that  $k$  is an integer in the interval  $1 \leq k \leq n$ , and by definition we have  $C^1 Z_{i_1} \equiv Z_{i_1}$ . The operation  $C^k Z_{i_1 i_2 \dots i_k}$  is easy to express in the computational basis since it produces a minus sign whenever the state  $|11\dots 1\rangle_{i_1 i_2 \dots i_k}$  is taken as input, i.e.  $C^k Z_{i_1 i_2 \dots i_k} |11\dots 1\rangle_{i_1 i_2 \dots i_k} = -|11\dots 1\rangle_{i_1 i_2 \dots i_k}$ , and leaves all the other states of the computational basis unchanged. Thus, every two operators of the  $C^k Z$  form always commute. Furthermore, as the action of the controlled  $Z$  gate is symmetric, it follows that the target qubit is not uniquely defined, but any of the  $k$  qubits on which  $C^k Z_{i_1 i_2 \dots i_k}$  acts can be thought of as the target one. We will exploit this property several times in the following, decomposing the gate in the most suitable way according to the context. It is also convenient to take  $C^0 Z \equiv -1$ , namely an overall minus

sign.

## 1.2 Standard graph states

In this section we introduce some basic concepts related to graph states, following Ref. [35]. This will be useful for both fixing the notation and introducing concepts that will be fundamental later.

Given a mathematical graph  $g_2 = \{V, E\}$ , i.e. a collection of  $n$  vertices  $V$  and some edges  $E$ , we can find the corresponding quantum state, the so-called graph state  $|g_2\rangle$  associated to the graph  $g_2$ , as follows:

1. Assign a qubit to each vertex.
2. Initialize each qubit to the state  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ . The initial state of the  $n$  qubits is then given by  $|+\rangle^{\otimes n}$ , which belongs to the set of REW states with  $f(x) = 0$  for every  $x$  (recall that, since the sign of  $|00\dots 0\rangle$  is chosen to be always positive, the constant function  $f(x) = 1$  is never considered here).
3. Wherever there is an edge, perform a controlled  $Z$  operation between the two connected qubits. Formally, if the qubits  $i_1$  and  $i_2$  are connected, then perform the operation  $C^2Z_{i_1i_2} = \text{diag}(1, 1, 1, -1)$  (expressed in the computational basis, as always considered in the following), where the superscript 2 stands for the number of qubits the operation acts on, while the subscripts  $i_1i_2$  represent the qubits involved. In the end, we get

$$|g_2\rangle = \prod_{\{i_1, i_2\} \in E} C^2Z_{i_1i_2} |+\rangle^{\otimes n}, \quad (1.3)$$

where  $\{i_1, i_2\} \in E$  means that the two vertices are connected by an edge.

This procedure can be explicitly sketched pictorially in Fig. 1.1, which clearly points out the correspondence.

We call the class of graph states as  $G_2$ , and a general state belonging to this set is denoted by  $|g_2\rangle$ . The subscript 2 is meant to recall that only two-body interactions of a given kind, represented by  $C^2Z$ , are considered in this case. The number of all possible graph states is given by  $2^{B(n,2)}$ , where  $B(n,2)$  is the binomial coefficient of  $n$  over 2. This number can be found as follows: given  $n$  vertices, the number of all possible edges is  $B(n,2)$ , therefore the number of all possible graphs, considering that each edge can be present or not, is  $2^{B(n,2)}$ .

We recall the reader that there exists a different, but equivalent, definition of graph states by exploiting the stabilizer formalism. The main idea is to define a set of operators, according to the graph, such that they uniquely define the graph state as the only state which is at the same time eigenstate



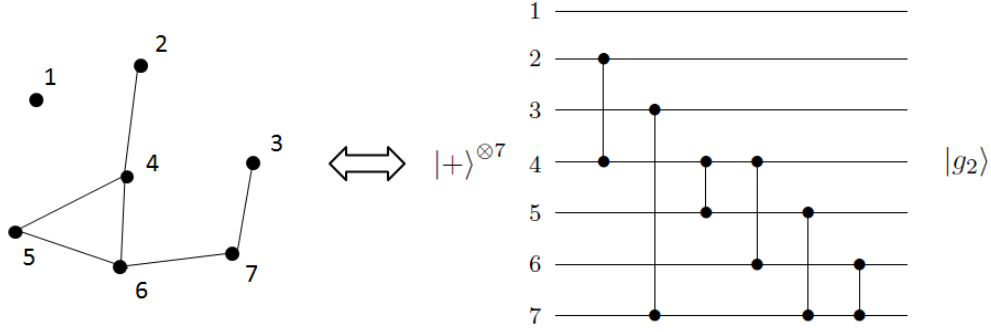


Figure 1.1: Correspondence between a mathematical graph and the quantum state associated to it. Since controlled- $Z$  gates are symmetric,  $C^2Z$  gates are here depicted as two dots connected by a vertical line. This notation will also be used for general controlled- $Z$  gates in the next figures.

of all of them with eigenvalue one. In a more formal way, for every vertex  $i$  we define the correlation operation  $K_i^{(2)}$  as follows

$$K_i^{(2)} = X_i \otimes Z_{N(i)} = X_i \bigotimes_{j \in N(i)} Z_j, \quad (1.4)$$

where  $N(i) = \{j | \{i, j\} \in E\}$  is the neighbourhood of the vertex  $i$ , namely the vertices  $j$  which are connected to  $i$  by an edge, and  $X$  and  $Z$  are the Pauli matrices  $\sigma_x$  and  $\sigma_z$ , respectively. The subscripts label the qubits on which the operators act. The set of  $n$  operators  $K_i^{(2)}$ ,  $\{K_i^{(2)}\}_{i=1,2,\dots,n}$ , uniquely defines the graph state  $|g_2\rangle$  associated to the graph, i.e.

$$K_i^{(2)} |g_2\rangle = |g_2\rangle \text{ for every } i = 1, 2, \dots, n. \quad (1.5)$$

It can be shown that the set  $\{K_i^{(2)}\}$  generates a commutative subgroup of the Pauli group on  $n$  qubits called stabilizer (as each element of the group stabilizes the state  $|g_2\rangle$ , see Eq. (1.5)) [35]. Recall that the Pauli group on a single qubit is defined as  $\{\pm \mathbb{1}, \pm i \mathbb{1}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ , which is generated by the three Pauli matrices alone  $\langle X, Y, Z \rangle$ . Notice that the Pauli group is trivially non commutative. The Pauli group on  $n$  qubits is then defined as the tensor product of operators belonging to the Pauli group of single qubits, for instance in the two-qubit case it is generated by  $\langle X_1, Y_1, Z_1, X_2, Y_2, Z_2 \rangle$ , thus by all Pauli matrices acting on either the first and the second qubit.

The definitions of graph states based on the explicit procedure involving  $C^2Z$  gates and on the stabilizer formalism can be shown to be equivalent [35].

With this in mind, we can now address the problem whether all REW states can be regarded as graph states and vice versa. A first hint that this is the case comes from the number of REW states versus graph states, i.e.  $2^{2^n-1}$  versus  $2^{B(n,2)}$ . Hence, disregarding local unitary equivalence, REW states are exponentially more many than graph states. Clearly, every graph state is also a REW state, since the action of  $C^2Z$  only produces some minus signs. However

the reverse does not hold. In order to prove this, we provide a counterexample given by the state

$$|f_G\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle), \quad (1.6)$$

which typically appears in Grover's algorithm. It is easy to show that the geometric measure of genuine multipartite entanglement [36] (defined in Eq. (2.3)) of the state above is  $E_2(|f_G\rangle) = 1/4$  [18], however every connected graph state of three qubits has a multipartite geometric measure  $E_2 = 1/2$  [37]. In conclusion graph states do not have such a rich structure as REW states, and thus they cannot provide a satisfactory description of the latter. Notice that, by construction, graph states only involve particular two-body interactions, which in this case turn out to be not sufficient to achieve all REW states. In order to overcome this problem, we introduce a wider class of states, namely hypergraph states. Let us start from  $k$ -uniform hypergraph states (a subset of the set of all hypergraph states), their definition will be given in a moment.

### 1.3 $k$ -uniform hypergraph states

In this section we generalize the notion of graph states allowing interactions which involve more than two parties. The mathematical tools needed to achieve this task are  $k$ -uniform hypergraphs. A  $k$ -uniform hypergraph  $g_k = \{V, E\}$  is a set of  $n$  vertices  $V$  with a set of edges  $E$ , where each edge connects exactly  $k$  vertices, and is called  $k$ -hyperedge (thus, a connected graph in the common sense is a 2-uniform hypergraph). An Example of a  $k$ -uniform hypergraph can be found on the LHS of Fig. 1.2.

Given a  $k$ -uniform hypergraph, by following an almost identical procedure as before, we can find the corresponding  $k$ -uniform hypergraph state as follows:

1. Assign a qubit to each vertex.
2. Initialise each qubit to the state  $|+\rangle$ . Notice that the preparing procedure is exactly the same as for graph states.
3. Wherever there is a  $k$ -hyperedge, perform a controlled  $Z$  operation between the  $k$  connected qubits. Formally, if the qubits  $i_1, i_2, \dots, i_k$  are connected, then perform the operation  $C^k Z_{i_1 i_2 \dots i_k}$ , where the superscript  $k$  stands for the number of qubits on which the operation acts, while the subscripts  $i_1 i_2 \dots i_k$  label the qubits involved. In the end, we get

$$|g_k\rangle = \prod_{\{i_1, i_2, \dots, i_k\} \in E} C^k Z_{i_1 i_2 \dots i_k} |+\rangle^{\otimes n}, \quad (1.7)$$

where  $\{i_1, i_2, \dots, i_k\} \in E$  means that the  $k$  vertices are connected by a  $k$ -hyperedge.

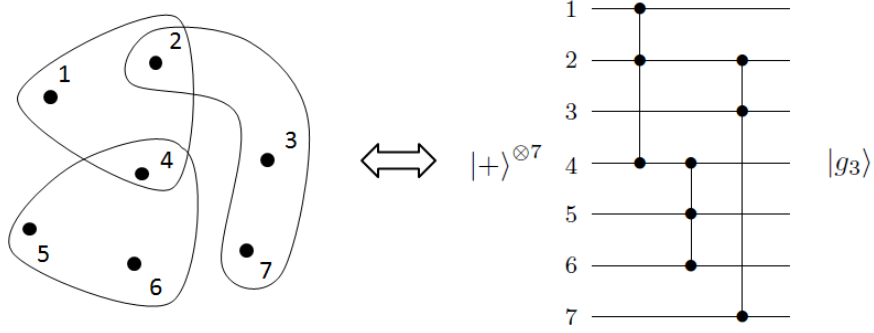


Figure 1.2: Correspondence between a mathematical 3-uniform hypergraph and the quantum state associated to it.

Once again, we refer the reader to Fig. 1.2, where the correspondence is explicitly restated in terms of the circuitual implementation of the corresponding quantum state.

Fixed  $k$ , we call the class of  $k$ -uniform hypergraph states as  $G_k$  and the general state out of it as  $|g_k\rangle$ . Notice that  $k$  is an integer ranging from 1 to  $n$ , namely  $1 \leq k \leq n$ . Let us have a look at the two extreme cases. The case  $k = 1$  can be recast as  $Z$  gates acting locally on single qubits, while the case  $k = n$  is the only one involving interaction among all  $n$  qubits, namely  $C^n Z_{i_1 i_2 \dots i_n}$ . Obviously, by setting  $k = 2$  we recover the class of standard graph states. The number of possible  $k$ -uniform hypergraph states is given by  $2^{B(n,k)}$ , therefore the most crowded classes are the ones where  $k$  is close to  $n/2$ .

At last, notice that the operations we perform, i.e.  $C^k Z_{i_1 i_2 \dots i_k}$ , are symmetric with respect to the computational basis, so that we do not need to care about which qubits represent the control and which the target. This is actually in accordance with our formalism with  $k$ -hyperedges.

As for standard graph states, a description in terms of the stabilizer formalism can be constructed as well. Just for the sake of simplicity, let us focus on 3-uniform hypergraph states, namely when three-body interactions  $C^3 Z$  are considered. For each vertex  $i$  we find the correlation operator defined as

$$K_i^{(3)} = X_i \otimes C^2 Z_{N(i)} = X_i \bigotimes_{(i_1, i_2) \in N(i)} C^2 Z_{i_1 i_2}, \quad (1.8)$$

where the neighbourhood of the vertex  $i$  is defined as  $N(i) = \{(i_1, i_2) | \{i, i_1, i_2\} \in E\}$ , which is a simple generalization of the concept of neighbourhood already introduced for graph states. Notice that now the neighbouring vertices are given by couples, instead of single vertices, as the interaction involves three different parties. As before, the set  $\{K_i^{(3)}\}_{i=1,2,\dots,n}$  defines the 3-uniform hypergraph state as the only one fulfilling the  $n$  constraints

$$K_i^{(3)} |g_3\rangle = |g_3\rangle \text{ for every } i = 1, 2, \dots, n. \quad (1.9)$$

Concerning the mathematical structure of the set  $\{K_i^{(3)}\}$ , we can still work out the group structure if we regard these  $n$  operators as generators of a group (see appendix A.1). The group then play the same role as before for standard graph states, stabilizing the state  $|g_3\rangle$ . However, in contrast with the stabilizer group of standard graph states, the group obtained in this case can no longer be regarded as a subgroup of the Pauli group, as it includes the  $C^2Z$  gate. Nevertheless the group is still Abelian, namely any two  $K_i^{(3)}$  and  $K_j^{(3)}$  defined according to Eq. (1.8) commute. The proof will be given for the larger set of hypergraph states (see appendix A.1), thus the commutativity of the stabilizers for 3-uniform hypergraphs will then follow as a special case.

In the general case where a  $k$ -uniform hypergraph is concerned, for each vertex  $i = 1, 2, \dots, n$  we can define a correlation operator given by

$$K_i^{(k)} = X_i \otimes C^{k-1} Z_{N(i)} = X_i \bigotimes_{(i_1, i_2, \dots, i_{k-1}) \in N(i)} C^{k-1} Z_{i_1 i_2 \dots i_{k-1}}, \quad (1.10)$$

where the neighbourhood  $N(i)$  of the vertex  $i$  is given by  $N(i) = \{(i_1, i_2, \dots, i_{k-1}) \mid \{i, i_1, i_2, \dots, i_{k-1}\} \in E\}$ , namely the set of  $k-1$ -tuples  $(i_1, i_2, \dots, i_{k-1})$  of vertices connected to  $i$  via  $k$ -hyperedges. The set of operators generated by  $\{K_i^{(k)}\}_{i=1,2,\dots,n}$  still form an Abelian group (see appendix A.1) which uniquely stabilizes a  $k$ -uniform hypergraph state. The unique  $k$ -uniform hypergraph state corresponding to the set  $\{K_i^{(k)}\}$  is then defined as the eigenvector with eigenvalue one of the  $n$  operators  $\{K_i^{(k)}\}$ , in formulae we have

$$K_i^{(k)} |g_k\rangle = |g_k\rangle \text{ for every } i = 1, 2, \dots, n. \quad (1.11)$$

Notice that in the special case of local interactions  $k = 1$  the definition (1.10) still works. Since we set  $C^0 Z = -1$  and the fact that  $X|-\rangle = -|-\rangle$ , the  $n$  operators given by Eq. (1.10) still stabilize the corresponding 1-uniform hypergraph state.

As for standard graph states, the definition following the stabilizer group is completely equivalent to the constructive procedure involving controlled  $Z$  operations on  $k$  qubits. The equivalence is explicitly derived in the most general case of non-uniform hypergraphs (see appendix A.2), whose  $k$ -uniform hypergraphs are a strict subset.

Before moving to the notion of general hypergraph states, let us conclude this section with the following note. The classification induced by  $k$ -uniformity allows us to prove that two sets  $G_k$  and  $G_{k'}$  cannot be connected by local Pauli operators for  $k \neq k'$  (apart from the trivial separable state  $|+\rangle^{\otimes n}$  which corresponds to the empty graph and thus is already contained in every class). Therefore, each set  $G_k$  gives rise to an inequivalent class under the action of the local Pauli group of  $n$  qubits (see appendix A.3). It is, however, an open question whether two sets  $G_k$  and  $G_{k'}$  with  $k \neq k'$  are inequivalent under the action of general local unitaries. An affirmative answer to this question would imply a corresponding multipartite entanglement classification.

## 1.4 Hypergraph states

In this section we conclude our ideal path by finding out what is a general hypergraph state, and eventually showing the one-to-one correspondence with REW states. Recall that this was our starting point.

Since we have already introduced the definition of  $k$ -uniform hypergraphs, the definition of a general hypergraph state follows trivially. A hypergraph is a collection of  $n$  vertices where hyperedges of any order  $k$  (thus  $k$  is no longer fixed but ranges from 1 to  $n$ ) are considered. The best way to understand this scenario is to have a look at Fig. 1.3, where the correspondence between the underlying mathematical hypergraph and the circuit implementation of the corresponding quantum state is explicitly pointed out. Notice that the starting state remains the same, i.e.  $|+\rangle^{\otimes n}$ , but now to each hyperedge corresponds a controlled  $C^k Z_{i_1 i_2 \dots i_k}$  where  $1 \leq k \leq n$ . For instance, in Fig. 1.3 hyperedges connecting 1, 2, 4 and 7 vertices appear, and thus controlled  $Z$  operations acting on 1, 2, 4 and 7 qubits must be considered. We recall the reader that the idea is essentially the same as for  $k$ -uniform hypergraph states, nevertheless hyperedges of different order can be present in the same graph now. We name the set of states produced in this way as  $G_{\leq n}$ , stressing that hyperedges connecting up to  $n$  vertices are present, and the general state belonging to this set as  $|g_{\leq n}\rangle$ . Given a mathematical hypergraph, the quantum state associated to it can be found by following three simple steps:

1. Assign a qubit to each vertex.
2. Initialise each qubit as  $|+\rangle$ , the total initial state is then  $|+\rangle^{\otimes n}$ .
3. Wherever there is a hyperedge, perform a controlled  $Z$  operation between the connected qubits. Formally, if the qubits  $i_1, i_2, \dots, i_k$  are connected by a  $k$ -hyperedge, then perform the operation  $C^k Z_{i_1 i_2 \dots i_k}$ . We eventually get the quantum state

$$|g_{\leq n}\rangle = \prod_{k=1}^n \prod_{\{i_1, i_2, \dots, i_k\} \in E} C^k Z_{i_1 i_2 \dots i_k} |+\rangle^{\otimes n}, \quad (1.12)$$

where  $\{i_1, i_2, \dots, i_k\} \in E$  means that the  $k$  vertices are connected by a  $k$ -hyperedge. Notice that the product on  $k = 1, 2, \dots, n$  accounts for different kinds of hyperedges that we can find in a general hypergraph.

It is worth of mention that this definition allows us to count the number of hypergraph states as any possible combination of  $k$ -uniform hypergraphs. As the number of the latter ones, fixed  $k$ , is given by  $2^{B(n,k)}$ , the total number of hypergraph states turns out to be

$$\prod_{k=1}^n 2^{B(n,k)} = 2^{\sum_{k=1}^n B(n,k)} = 2^{2^n - 1}. \quad (1.13)$$

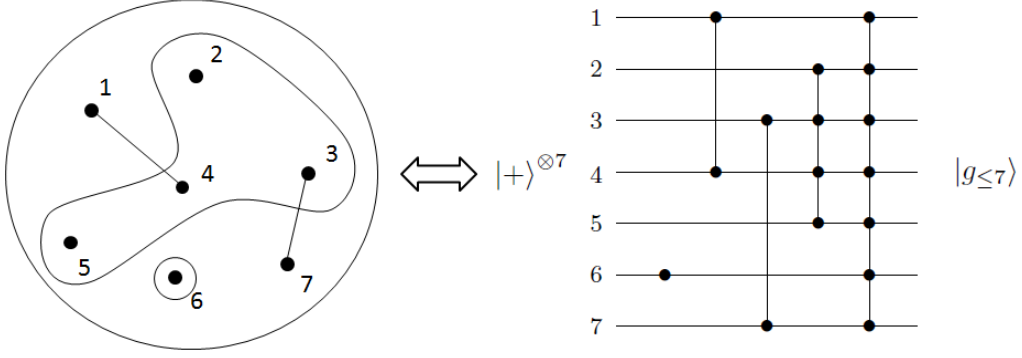


Figure 1.3: Correspondence between a mathematical hypergraph and the quantum hypergraph state. The circle around vertex 6 stands for a local  $Z$  gate, corresponding to a hyperedge of order  $k = 1$ , while the big circle around all vertices corresponds to a full-body interaction.

Surprisingly (or not) this is exactly the number of states belonging to the REW set, hence the counting hints that we are going in the right direction. However, despite this noticeable coincidence, we still need to check whether any REW state can be interpreted as a hypergraph state and vice versa. Before proving our main result we would like to spend a few words on the stabilizer formalism in this general scenario.

Given a completely general hypergraph, for any vertex  $i$  we define the following correlation operator

$$K_i = X_i \otimes \prod_{k=1}^n C^{k-1} Z_{N(i)} = X_i \prod_{k=1}^n \bigotimes_{(i_1, i_2, \dots, i_{k-1}) \in N(i)} C^{k-1} Z_{i_1 i_2 \dots i_{k-1}}, \quad (1.14)$$

where the product over  $k$  still takes into account that hyperedges of different orders are considered. For any value of  $k$ , the neighbourhood  $N(i)$  of the vertex  $i$  is defined as  $N(i) = \{(i_1, i_2, \dots, i_{k-1}) | \{i, i_1, i_2, \dots, i_{k-1}\} \in E\}$ . Different kinds of neighbourhoods can obviously appear in this scenario (single vertices, couples and in general  $k-1$ -tuples), depending on the order  $k$  of the hyperedges that the vertex  $i$  shows. For instance, in Fig. 1.3 the neighbourhoods  $N(4)$  of vertex 4 are the sets 1, (2, 3, 5) and (1, 2, 3, 5, 6, 7), since the vertex is connected via 2-, 4- and 7-hyperedges. We would like to stress that, even though the  $n$  correlation operators defined above seem more complicated than the ones found for  $k$ -uniform hypergraphs, they are meant exactly in the same spirit. It is just a matter of notation which inevitably becomes slightly heavier.

The question is now whether the operators  $\{K_i\}_{i=1,2,\dots,n}$  defined in Eq. (1.14) show some nice mathematical properties. It can be shown (see appendix A.1) that the set  $\{K_i\}$  still generates an Abelian group which uniquely stabilizes the hypergraph state. The hypergraph state corresponding to the set  $\{K_i\}$  is then defined as the unique eigenvector with eigenvalue one of every generator  $K_i$ , in formulae

$$K_i |g_{\leq n}\rangle = |g_{\leq n}\rangle \text{ for every } i = 1, 2, \dots, n. \quad (1.15)$$

Furthermore, it turns out (see appendix A.2) that the definition according to the stabilizer formalism is equivalent to the one in terms of controlled  $Z$  gates. Therefore, having proved that this holds in the most general scenario of hypergraph states, namely where  $k$ -hyperedges of any order  $1 \leq k \leq n$  are present, we have automatically proved it for  $k$ -uniform hypergraph states (notice that also standard graph states, i.e.  $k = 2$ , are included).

### 1.5 Equivalence between hypergraph and REW states

We are now ready to state our main result: the set  $G_{\pm}$  of REW states and the set  $G_{\leq n}$  of hypergraph states coincide. The direction  $G_{\leq n} \subseteq G_{\pm}$  follows trivially, since any  $|g_{\leq n}\rangle$  is obtained from  $|+\rangle^{\otimes n}$  by applying controlled  $Z$  gates whose action is just to create some minus signs in front of the states of the computational basis. The other direction  $G_{\pm} \subseteq G_{\leq n}$  is not so trivial but can be proved by the following constructive approach. Suppose we are given a REW state  $|f\rangle$ , then the following procedure leads to the underlying hypergraph:

1. Every time  $|f\rangle$  has a minus sign in front of the components of the computational basis with one excitation, i.e. of the form  $|0\dots 01_k 0\dots 0\rangle$ , apply local  $Z$  operations. Doing so, we erase the right minus signs in front of the components with one excitation, but nevertheless we create many other unnecessary minuses in front of components with more than one excitations.
2. Apply now  $C^2Z$  gates in order to erase the negative signs in front of the components with two excitations. Notice that these minuses are either from the original state  $|f\rangle$  or as by products of the previous step. The key point is that the minus signs previously erased (i.e. the ones in front of the single-excitation states) remain untouched, since  $C^2Z$  acts non-trivially on states with at least two excitations.
3. As a general rule, apply  $C^kZ$ , from  $k = 1$  till  $k = n$ , erasing subsequently the minus signs in front of the components of the computational basis. In general, at the step  $k$  we will be able to erase the minus signs in front of the states with up to  $k$  excitations.
4. Consider the collection of gates that you need to bring  $|f\rangle$  back to  $|+\rangle^{\otimes n}$ , this provides the hypergraph associated to the regarded REW state.

Notice that, even though the final collection of controlled  $Z$  gates is composed of commuting operators, the proof is actually based on an ordered procedure, namely at each step we consider gates acting on one more qubit than in the previous step. This is an essential ingredient, otherwise we could change the signs already fixed. Furthermore, since the procedure is uniquely defined according

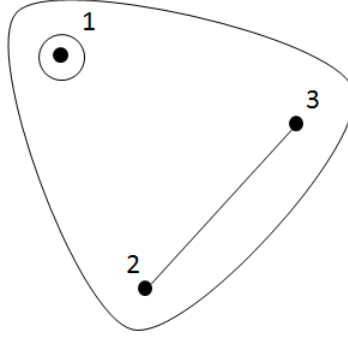


Figure 1.4: Hypergraph corresponding to the REW state given by Eq. (1.16).

to the REW state from which we start, the underlying hypergraph is unique. Therefore, the correspondence between the sets  $G_{\pm}$  and  $G_{\leq n}$  is one-to-one.

Just to fix the ideas, let us consider the explicit example of the three-qubit REW state given by

$$\frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle). \quad (1.16)$$

The task is to find out the underlying hypergraph state by following the explicit procedure explained above. It is straightforward to see that the following chain of states leads to the initial state  $|+\rangle^{\otimes 3}$ :

$$\begin{aligned} & \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle), \\ & \quad \downarrow Z_1 \\ & \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle), \\ & \quad \downarrow C^2 Z_{23} \\ & \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle), \\ & \quad \downarrow C^3 Z_{123} \\ & \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle). \end{aligned}$$

Therefore the hypergraph corresponding to the REW state of Eq. (1.16) is the one drawn in Fig. 1.4.

Other interesting examples are REW states employed in quantum algorithms. In Grover's algorithm for instance, REW states with only one minus sign appear, such as the state (1.6) for three qubits (the minus sign marks the single solution of the search problem). It is easy to see that, when the number of minus signs is odd, the REW state always involves a controlled  $Z$  gate acting on all the qubits, therefore involving  $n$ -body interactions. On the contrary, for REW states employed in Deutsch-Jozsa's algorithm, such a gate is never needed, since the function  $f$  is either constant or balanced (balanced means that the number of minus signs equals the number of plus signs), while the application of a controlled  $Z$  gate acting on all qubits would change just one sign in the  $n$ -qubit state, therefore necessarily leading to an unbalanced



function. An explicit example of a balanced state is given by modifying the state in Eq. (1.16) such that a plus sign is placed in front of the component  $|111\rangle$ . Such a state would be generated by a sequence of the  $Z_1$  and the  $C^2Z_{23}$  gates, without the application of  $C^3Z_{123}$ .

### 1.6 Comments and future work

In conclusion, we have introduced the class of quantum hypergraph states, which are associated to corresponding mathematical hypergraphs and are stabilized by non local observables. We have shown that there is a one-to-one correspondence between the set of hypergraph states and the set of real equally weighted states, which are essential for quantum algorithms. A constructive method was introduced which allows us to generate the hypergraph underlying a given real equally weighted state, i.e. a quantum state encoding a Boolean function  $f$ . We have discussed the types of many-body interactions needed to generate general hypergraph states in a Hamiltonian description, going beyond the two-body interaction that characterises graph states.

For future studies, since the class of hypergraph states naturally generalizes the class of graph states, it is of great interest to ask whether some of the many results about the latter, such as for instance measurement-based quantum computing [38], entanglement witnessing [37], and quantum error correcting techniques [39, 40], can be extended to the former. Some achievement in this sense already exists, mainly related to purification protocols [41]. Furthermore, this larger class of states may enable even more applications and quantum protocols, especially in connection to already existing algorithms employing hypergraphs, as e.g. the 3-SAT problem [42].

# Entanglement in Grover's Algorithm

Even though entanglement is considered as a major resource in quantum information processing, the role it plays in achieving the quantum computational speed-up in the currently known quantum algorithms is not yet fully understood. In Ref. [7] it was shown that in Shor's algorithm multipartite entanglement is needed to achieve exponential computational speed-up with quantum resources. More recently, it was shown that multipartite entangled states are employed in the Deutsch-Jozsa algorithm and in the first step of the Grover algorithm [8, 17]. Moreover, multipartite entanglement was shown to be present at each computational step in Grover's algorithm and a scale invariance property of entanglement dynamics was proved [18].

In this chapter we review in a unified way the results presented in Refs. [17, 18] for Grover's algorithm. We firstly analyse in detail the entanglement content of the initial states of the Grover algorithm, and show how they can be expressed in terms of hypergraphs. Then, we calculate the amount of entanglement of the multiqubit quantum states employed in the whole algorithm, by following its dynamics at each step of the computation. Genuine multipartite entanglement is shown to be always present. Remarkably, the dynamics of any type of entanglement as well as of genuine multipartite entanglement is independent of the number  $n$  of qubits for large  $n$ , thus exhibiting a scale invariance property. We compare this result with the entanglement dynamics induced by a fixed-point quantum search algorithm, and finally investigate criteria for efficient simulatability in the context of the standard Grover search.

## 2.1 Some remarks about Grover's algorithm

Let us remind the reader that the Grover search algorithm [3] employs pure states of  $n$  qubits which are initially prepared in  $|\psi_0\rangle$  of Eq. (1.1), namely an equally weighted superposition of all computational basis states. The initial

## 2. Entanglement in Grover's Algorithm

---

state  $|\psi_0\rangle$  can be more conveniently written as

$$|\psi_0\rangle = \sqrt{\frac{N-M}{N}} |X_0\rangle + \sqrt{\frac{M}{N}} |X_1\rangle, \quad (2.1)$$

where  $N = 2^n$  and  $M$  is the number of searched items (in the following also referred to as “solutions” of the search problem). Here,  $|X_1\rangle = \frac{1}{\sqrt{M}} \sum_{x_s} |x_s\rangle$  represents the superposition of all the states  $|x_s\rangle$  that are solutions (i.e. searched items), and  $|X_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{x_n} |x_n\rangle$  denotes the superposition of all the states  $|x_n\rangle$  that are not searched for. The global state after  $k$  iterations of the Grover operation  $G$  has the form [1, 43]

$$|\psi_k\rangle \equiv G^k |\psi_0\rangle = \cos \theta_k |X_0\rangle + \sin \theta_k |X_1\rangle, \quad (2.2)$$

with  $\theta_k = (k + 1/2)\theta$  and  $\theta = 2\sqrt{M/N}$  in the limit  $M \ll N$ . The unitary operation  $G$  is usually decomposed into two basic blocks,  $G = \mathcal{I} \circ U_f$ , where  $U_f$  represents the oracle call, i.e.  $U_f = \mathbb{1} - 2 |X_1\rangle \langle X_1|$ , and  $\mathcal{I}$  is the inversion about the mean operation, namely  $\mathcal{I} = -(\mathbb{1} - 2 |\psi_0\rangle \langle \psi_0|)$ . The operation  $G$  is repeated until the state  $|\psi_k\rangle$  overlaps as much as possible with  $|X_1\rangle$ , namely for  $k_{opt} = CI[(\pi/\theta - 1)/2]$ , where  $CI[x]$  denotes the closest integer to  $x$ . In the limit  $M \ll N$ , the optimal number of iterations is  $k_{opt} = CI[\frac{\pi}{4} \sqrt{N/M} - \frac{1}{2}]$ , i.e. it is proportional to the square root of  $N$ . In the following we will consider the condition  $M \ll N$  to be always fulfilled.

### 2.2 Entanglement content of initial states in Grover's algorithm

We now study the entanglement properties of the initial states  $|f_G\rangle = U_f |\psi_0\rangle$ , i.e. the states created at the beginning of the Grover algorithm just after the action of the oracle  $U_f$ , in terms of the number of qubits  $n$  for a fixed small number of solutions,  $M = 1, 2$ . Remember that the state  $|f_G\rangle$  is given by Eq. (1.2), where the Boolean function is now defined such that  $f_G(x) = 1$  if  $x$  is a solution of the search problem, and  $f_G(x) = 0$  otherwise. The search problem then reduces to find the strings that, input to  $f_G$ , give the value one as output. Notice that, since we consider a small number of solutions, then the state  $|f_G\rangle$  is apparently very similar to  $|\psi_0\rangle$ , as only some minus signs appear. However, the presence of these few minus signs will make a big difference in the entanglement content of the Grover initial state  $|f_G\rangle$  with respect to  $|\psi_0\rangle$ .

We quantify the amount of entanglement by the geometric measure of entanglement (GME) [36], which for a pure  $n$ -partite state  $|\psi\rangle$  reads

$$E_q(|\psi\rangle) = 1 - \max_{|\phi\rangle \in S_q} |\langle \psi | \phi \rangle|^2, \quad (2.3)$$

where  $S_q$  is the set of  $q$ -separable states, namely states that are separable for  $q$  partitions of the  $n$ -qubit system. The GME represents a suitable entanglement measure when multipartite systems are taken into account. Notice that

$E_n$  quantifies the amount of entanglement of any kind contained in the global system, i.e. it is non-vanishing even for states showing entanglement just between two subsystems, while  $E_2$  quantifies genuine multipartite entanglement [44]. In the section we restrict ourselves to the evaluation of  $E_n$  only.

### 2.2.1 Single solution

Let us first consider the case of a single solution to the search problem ( $M = 1$ ). Without loss of generality, as will be proved later, we consider the state representing the solution to be invariant under any permutation of the  $n$  qubits (e.g.  $|111\dots 1\rangle$ ). Therefore, the state  $|f_{M=1}\rangle$  after the oracle call is given by

$$|f_{M=1}\rangle = \frac{1}{\sqrt{2^n}} \left( \sum_{x=0}^{2^n-1} |x\rangle - 2|1\dots 11\rangle \right), \quad (2.4)$$

and it is also permutation invariant. Let us first compute  $E_n$  for the above state for varying  $n$ . Due to the symmetry property, the search for the maximum in Eq. (2.3) can be restricted to symmetric separable states  $|\phi\rangle^{\otimes n}$  [45], so that the maximization involves only the two parameters  $\alpha \in [0, \pi]$  and  $\beta \in [0, 2\pi]$  that define the single-qubit state  $|\phi\rangle = \cos \frac{\alpha}{2} |0\rangle + e^{i\beta} \sin \frac{\alpha}{2} |1\rangle$ .

The GME  $E_n$  for a single solution then takes the form

$$E_n(|f_{M=1}\rangle) = 1 - \max_{\alpha, \beta} \frac{1}{2^n} \left| \left( \cos \frac{\alpha}{2} + e^{i\beta} \sin \frac{\alpha}{2} \right)^n - 2e^{i\beta} \sin \frac{\alpha}{2} \right|^2. \quad (2.5)$$

The optimal value of  $\beta$  can be shown to be zero by induction over the number  $n$  of qubits, while the optimal  $\alpha$  can be found by setting  $t = \tan \frac{\alpha}{2}$  and calculating the derivative of the overlap explicitly, which reduces to finding the root of a polynomial in  $t$ .

In Fig. 2.1 we report the behaviour of  $E_n(|f_{M=1}\rangle)$ . As we can see, the amount of entanglement decreases exponentially for increasing number of qubits. This fact has a very intuitive explanation. As  $n$  increases, the number of states composing the computational basis increases exponentially, while the number of solution is fixed as constant  $M$ , thus the ratio  $M/2^n$  becomes exponentially smaller. So, in the limit of infinitely many qubits, the state shows a vanishing amount of entanglement, cause it becomes indistinguishable from the fully separable state  $|\psi_0\rangle$ . Notice nevertheless that, as the state  $|f_{M=1}\rangle$  has an odd number of minus signs, even though the state shows an infinitely small amount of entanglement  $E_n$ , the results in Ref. [8] guarantee that the involved entanglement is actually genuine multipartite.

We point out that all the results explicitly derived for permutation invariant states hold also for any Grover search with one searched item. Actually, all these states can be achieved from the symmetric one by applying tensor products of  $\sigma_x$  Pauli operators and identity operators  $\mathbb{1}$  (e.g.  $|001\dots 1\rangle = \sigma_x \otimes \sigma_x \otimes \mathbb{1} \dots |111\dots 1\rangle$ ). Since these operations are local, they obviously do not change the entanglement content of the resulting state.

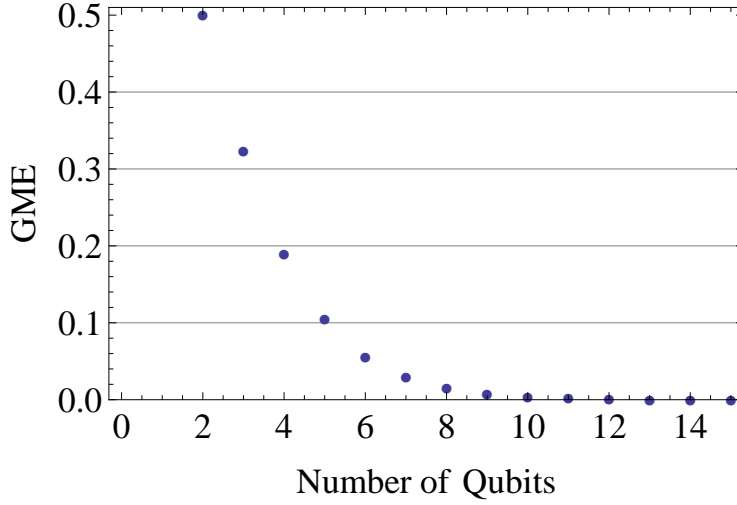


Figure 2.1: The GME  $E_n(|f_{M=1}\rangle)$  as a function of the number of qubits  $n$  composing the register, for a single searched item.

### 2.2.2 Two solutions

Let us now focus on the states employed in the case of two solutions of the search problem  $|f_{M=2}\rangle$ , i.e. states of the form (1.2) with two minus signs. We introduce a sort of classification of these states based on the Hamming distance  $d$  between the two computational basis states representing the solutions. We will show that the entanglement properties of the regarded states depend crucially on the number of digits in which the two solutions differ, i.e. on their Hamming distance  $d$ .

Without loss of generality, as will be proved below, we consider first the case in which the two  $n$ -qubit states representing the solutions differ in the first  $d$  digits and are invariant under permutations of the first  $d$  and last  $n-d$  qubits, respectively (e.g.  $|\underbrace{0\dots 0}_d 1\dots 1\rangle$  and  $|\underbrace{1\dots 1}_d 1\dots 1\rangle$ ), i.e.

$$|f_{M=2}\rangle = \frac{1}{\sqrt{2^n}} \left( \sum_{x=0}^{2^n-1} |x\rangle - 2(|\underbrace{0\dots 0}_d 1\dots 1\rangle + |\underbrace{1\dots 1}_d 1\dots 1\rangle) \right). \quad (2.6)$$

We first compute  $E_n$  for this set of states for varying  $n$ . Due to the permutation invariance property, the search for the GME  $E_n$  can still be restricted to separable states that show the same symmetry [45], i.e.  $|\phi\rangle^{\otimes d} |\varphi\rangle^{\otimes n-d}$ . Therefore the maximization involves only the four parameters  $\alpha, \gamma \in [0, \pi]$  and  $\beta, \delta \in [0, 2\pi]$  that define the two single-qubit states  $|\phi\rangle$  and  $|\varphi\rangle$ .

The GME  $E_n$  for two solutions with Hamming distance  $d$  then takes the

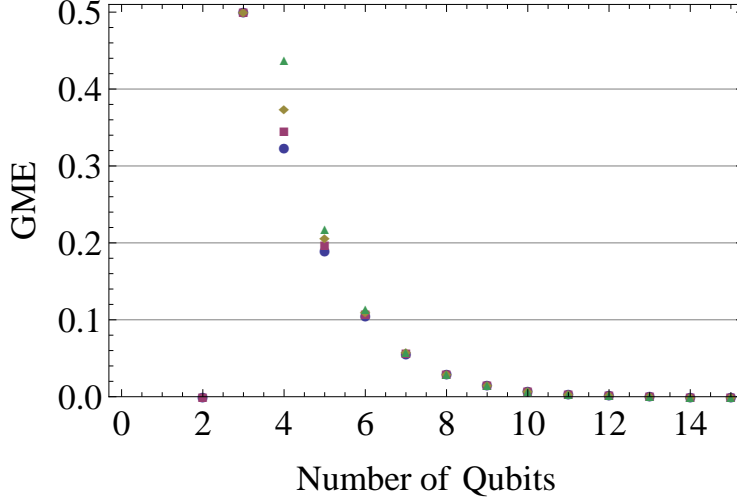


Figure 2.2: The GME  $E_n(|f_{M=2}\rangle)$  as a function of the number of qubits  $n$  composing the register, for two searched items. Several Hamming distances  $d$  are plotted for a comparison:  $d = 1$  blue dots,  $d = 2$  purple squares,  $d = 3$  yellow diamonds,  $d = 4$  green triangles. Notice that the state of two qubits is always separable for both  $d = 1, 2$  and that  $E_n(|f_{M=2}\rangle)$  for three qubits collapses to the single value  $1/2$ .

form

$$E_n(|f_{M=2}\rangle) = 1 - \max_{\alpha, \beta, \gamma, \delta} \frac{1}{2^n} \left| \left( \cos \frac{\alpha}{2} + e^{i\beta} \sin \frac{\alpha}{2} \right)^d \left( \cos \frac{\gamma}{2} + e^{i\delta} \sin \frac{\gamma}{2} \right)^{n-d} - 2e^{i(n-d)\delta} \sin^{n-d} \frac{\gamma}{2} \left( \cos^d \frac{\alpha}{2} + e^{id\beta} \sin^d \frac{\alpha}{2} \right) \right|^2. \quad (2.7)$$

Notice that when  $d = n$  the maximization procedure involves only two parameters. This can be easily explained by noticing that in this case the state turns out to be completely invariant under any permutation of the qubits, and thus only two parameters are needed.

As before, the optimal parameters  $\alpha$ ,  $\beta$ ,  $\gamma$  and  $\delta$  can be computed by maximizing the squared overlap numerically. The obtained results are shown in Fig. 2.2 where the GME is plotted versus the number of qubits composing the register. As in the case  $M = 1$ , we can see that  $E_n$  approaches zero exponentially fast for increasing  $n$ . It is worth mentioning that this behaviour holds for any value of the Hamming distance  $d$ , so in the limit of large  $n$ , the GME depends only slightly on  $d$ . This is however not the case if one considers a finite number  $n$  of qubits, as can be clearly seen in Fig. 2.2. The higher the Hamming distance is, the more entangled the state is. Therefore, in this case the Hamming distance plays a crucial role for the amount of entanglement, since states with two solutions with higher distance  $d$  exhibit a higher amount of entanglement.

## 2. Entanglement in Grover's Algorithm

---

At last, notice that all the results presented so far, even if they were explicitly derived for partially permutation invariant states, hold for any Grover search with two searched items, i.e.  $M = 2$ . Actually, analogously to the case of a single solution previously discussed, also for  $M = 2$  all of these states with fixed Hamming distance  $d$  can be reached from a partially symmetric one by applying tensor products of  $\sigma_x$  Pauli operators and identity operators  $\mathbb{1}$  and/or permutations of the  $n$  qubits. Again, since these operations are local, they do not change the entanglement content of the resulting state.

### 2.2.3 Connection to hypergraph states

Quantum hypergraph states introduced in the previous chapter allow us to describe the initial states employed in the Grover algorithm in a very convenient way. Indeed the kind of entanglement and the gates (of the  $CZ$  type) that we need in order to create them experimentally will emerge very easily from their hypergraph structure.

Consider firstly the initial symmetric state  $|f_{M=1}\rangle$  given by Eq. (2.4). It is then straightforward to see that it corresponds to the hypergraph where the single hyperedge involving all vertices is drawn. Therefore, it has a very simple structure in the light of hypergraphs, but a very different entanglement content from standard graph states.

In order to discuss the case with two minus signs, let us first notice that the total hyperedge of order  $n$  never appears now, since we are dealing with an even number of minus signs. Hence, even though states  $|f_{M=2}\rangle$  of Eq. (2.6) might have a much more complicated graph structure than  $|f_{M=1}\rangle$ , the gate  $C^n Z$  is never involved to create them. Just for the sake of simplicity, let us focus on the specific case of four qubits, the general result for  $n$  qubits will be stated later.

The hypergraphs corresponding to the four-qubit symmetric states  $|f_{M=2}\rangle$  with Hamming distance  $d = 1, 2, 3$  and 4 are shown in Fig. 2.3. When  $d = 1$  the underlying hypergraph is the one where only the vertices 2, 3 and 4 are connected by a 3-hyperedge. Thus, the biseparability of the state with respect to the bipartition  $1|234$  follows immediately. On the other hand, when  $d = 3$  the hypergraph is given by connecting the vertex 4 to the other three vertices in any possible way, i.e. exploiting any possible hyperedge. Notice instead that the case  $d = 4$  must be recast to the case with a plus sign in front of the computational basis state  $|0\dots 00\rangle$  by multiplying all amplitudes by a factor  $-1$ . As a result it is now not so difficult to show that the corresponding hypergraph is the one with all possible hyperedges, apart from the total one  $C^4 Z$ . Thanks to the above discussion we can state the general rule for the initial multiqubit states  $|f_{M=2}\rangle$  with general Hamming distance  $d$ .

Let  $(\underbrace{|0\dots 0\rangle}_d + \underbrace{|1\dots 1\rangle}_d)\underbrace{|1\dots 1\rangle}_{n-d}$  be the only two states with a negative phase in the superposition  $|f_{M=2}\rangle$ , then the hypergraph related to  $|f_{M=2}\rangle$  can be found as follows:

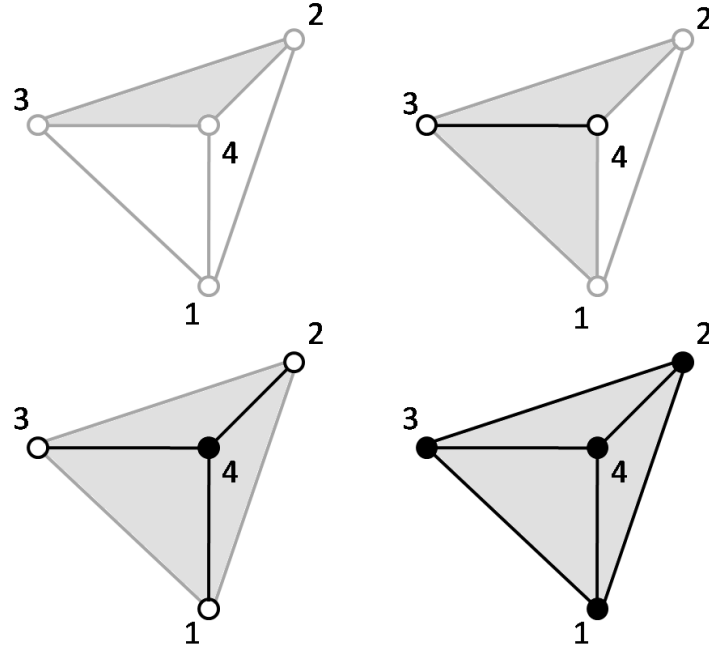


Figure 2.3: Hypergraphs associated to the four-qubit initial Grover states with two solutions for several values of the Hamming distance. Top-left corner:  $d = 1$ , top-right corner:  $d = 2$ , bottom-left corner:  $d = 3$ , and bottom-right corner:  $d = 4$ . Each empty vertex represents a qubit. Full dark dots, dark lines and grey faces represent hyperedges of order 1, 2 and 3, respectively. Notice that in the hypergraph with  $d = 4$  also the hidden face connecting the vertices 1, 2 and 3 is present.

1. Group the last  $n - d$  vertices with a hyperedge of order  $n - d$ .
2. Connect the whole group to the remaining  $d$  vertices in any possible way, namely by exploiting hyperedges of any order greater than  $n - d$ . Remember not to use the hyperedge of order  $n$ .

Notice that both the extreme cases  $d = 1$  and  $d = n$  fit into this scheme. Regarding the former, since we are not allowed to draw the hyperedge of order  $n$ , we are left with a biseparable hypergraph. Instead, for the latter we do not apply the first step of the procedure above, but we nevertheless connect all possible vertices according to the second step.

## 2.3 Entanglement dynamics in Grover's algorithm

In this section we study the entanglement properties of the states (2.2) in terms of the number of iterations  $k$  and the number of qubits  $n$  for a fixed number of solutions. We still quantify the amount of entanglement by the



GME defined in Eq. (2.3), calculating both  $E_n$  and  $E_2$  at every step  $k$  of the Grover algorithm. As before, we focus on the two simple cases of a single and two solutions, namely  $M = 1, 2$ .

### 2.3.1 Single solution

Let us first consider the case of a single solution to the search problem ( $M = 1$ ). As done in the previous section, we consider the state  $|X_1\rangle$  representing the solution to be invariant under any permutation of the  $n$  qubits (e.g.  $|11\dots 1\rangle$ ). Therefore, the state  $|\psi_{k,M=1}\rangle$  at the step  $k$  of the algorithm is also permutation invariant for all  $k$ 's. Let us first compute  $E_n$  for this set of states for varying  $k$ . Due to this symmetry property, the search for the maximum in Eq. (2.3) can still be restricted to symmetric separable states  $|\phi\rangle^{\otimes n}$  [45], so that the maximization involves only the two parameters  $\alpha \in [0, \pi]$  and  $\beta \in [0, 2\pi]$  that define the state  $|\phi\rangle$ . Furthermore, since  $\theta_k \in [0, \pi/2]$  the coefficients of  $|\psi_k\rangle$ , defined in Eq. (2.2), are all positive and the optimal value of the phase factor can be fixed to  $\beta = 0$ . The GME  $E_n$  for a single solution then takes the form

$$E_n(|\psi_{k,M=1}\rangle) = 1 - \max_{\alpha} \left| \frac{\cos \theta_k}{\sqrt{2^n - 1}} \left[ \left( \cos \frac{\alpha}{2} + \sin \frac{\alpha}{2} \right)^n - \sin^n \frac{\alpha}{2} \right] + \sin \theta_k \sin^n \frac{\alpha}{2} \right|^2 \quad (2.8)$$

The optimal value of  $\alpha$  can then be found by setting  $t = \tan \frac{\alpha}{2}$  and calculating the derivative of the overlap explicitly, which reduces to finding the root of a polynomial in  $t$ .

In Fig. 2.4 we report the behaviour of  $E_n(|\psi_{k,M=1}\rangle)$  for  $n = 12$ : the entanglement increases in the first half of iterations, achieves the maximal value of about  $1/2$ , and then decreases to zero as soon as the optimal number of iterations is reached. This behaviour is qualitatively similar to the ones shown in [46, 47], where the dynamics of both the two-qubit concurrence and the Von Neumann entropy of the half-qubit reduced state was studied.

In order to quantify only genuine multipartite entanglement we now calculate  $E_2$ . The expression of  $E_2(|\psi\rangle)$  can be rewritten as [48]

$$E_2(|\psi\rangle) = 1 - \max_P \max_{\mu} \mu^2, \quad (2.9)$$

where the  $\mu$ 's are the Schmidt coefficients of  $|\psi\rangle$  with respect to a fixed bipartition  $P|Q$ , and  $\max_P$  denotes the maximization over all possible bipartitions. Notice that, since the regarded state  $|\psi_{k,M=1}\rangle$  is permutation invariant, we need to check only  $\lfloor n/2 \rfloor$  bipartitions, where  $\lfloor x \rfloor$  is the largest integer smaller or equal to  $x$ . In order to find the maximal Schmidt coefficient of  $|\psi_{k,M=1}\rangle$  among all possible bipartitions we fix a generic bipartite splitting  $P|Q$ , where  $P$  is composed of  $m$  qubits and  $Q$  of the remaining  $n - m$ , and compute the eigenvalues of the reduced density operator  $\rho_P = \text{Tr}_Q[|\psi_{k,M=1}\rangle \langle \psi_{k,M=1}|]$ , given

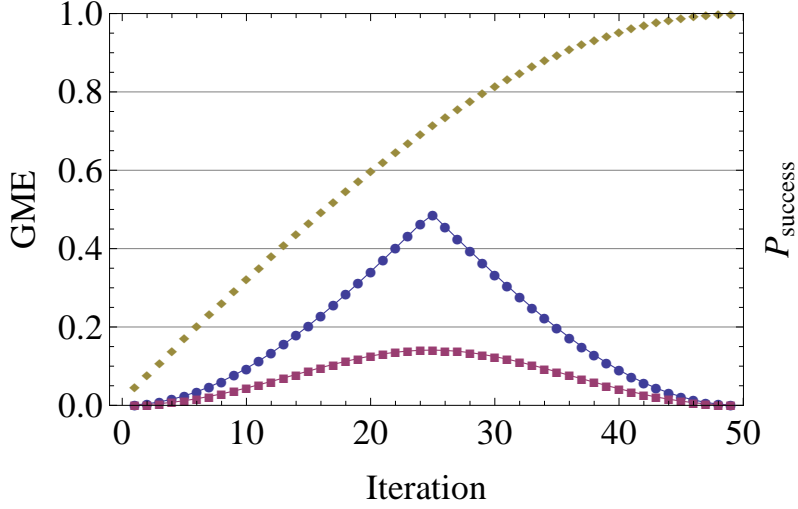


Figure 2.4: Evolution of entanglement as a function of the number of steps  $k$ , for a single searched item, with  $n = 12$  qubits and  $k_{opt} = 49$ .  $E_n(|\psi_{k,M=1}\rangle)$  is depicted by blue dots, while  $E_2(|\psi_{k,M=1}\rangle)$  by purple squares. The yellow dots represent the success probability.

by the following  $2^m \times 2^m$  matrix

$$\rho_P = \begin{pmatrix} a & \dots & a & b \\ \vdots & \ddots & \vdots & \vdots \\ a & \dots & a & b \\ b & \dots & b & c \end{pmatrix}, \quad (2.10)$$

where  $a = 2^{n-m}A^2$ ,  $b = a - A(A - B)$ , and  $c = a - A^2 + B^2$ , with  $A = \cos \theta_k / \sqrt{2^n - 1}$  and  $B = \sin \theta_k$ . The maximal eigenvalue of the above matrix can be explicitly calculated (see Appendix B.1), and it is given by

$$\lambda_{max} = \frac{1}{2} + \frac{1}{2} \left[ 1 - 4(2^m - 1)(2^{n-m} - 1)A^2(A - B)^2 \right]^{\frac{1}{2}}. \quad (2.11)$$

By deriving the above expression with respect to  $m$ , it is easy to show that the bipartition that leads to the maximum eigenvalue corresponds to  $m = 1$  for all values of  $k$ . According to Eq. (2.9), then the multipartite GME  $E_2$  takes the explicit form

$$E_2(|\psi_{k,M=1}\rangle) = \frac{1}{2} - \frac{1}{2} \left[ 1 - 4 \frac{2^{n-1} - 1}{2^n - 1} \cos^2 \theta_k \left( \frac{\cos \theta_k}{\sqrt{2^n - 1}} - \sin \theta_k \right)^2 \right]^{\frac{1}{2}}. \quad (2.12)$$

This result shows that genuine multipartite entanglement has a qualitative similar behaviour as  $E_n(|\psi_{k,M=1}\rangle)$  (see Fig. 2.4), even if it achieves a maximum of about 0.14 and the curve is derivable in that point. Notice also that  $E_2(|\psi_{k,M=1}\rangle)$  is symmetric with respect to  $k_{opt}/2$ .

## 2. Entanglement in Grover's Algorithm

---

We now show that the entanglement dynamics in the Grover algorithm, namely the behaviour of  $E_n$  and  $E_2$  during the operation of the algorithm, does not depend on the number of qubits  $n$ , thus exhibiting the property of scale invariance. For  $2^n \gg 1$  the two entanglement measures take the simple forms (see Appendix B.2 for the detailed calculation)

$$\begin{aligned} E_n(|\psi_{k,M=1}\rangle) &\simeq \begin{cases} \sin^2 \theta_k & \text{for } \theta_k \leq \pi/4, \\ \cos^2 \theta_k & \text{for } \theta_k > \pi/4, \end{cases} \\ E_2(|\psi_{k,M=1}\rangle) &\simeq \frac{1}{2} \left[ 1 - \left( 1 - \frac{1}{2} \sin^2 2\theta_k \right)^{\frac{1}{2}} \right]. \end{aligned} \quad (2.13)$$

Both expressions depend only on  $\theta_k \simeq \frac{\pi}{2} k/k_{opt}$ , namely on  $k/k_{opt}$ , and not on  $k$  and  $n$  separately. Therefore, the entanglement dynamics of the Grover algorithm is scale invariant in the sense that it only depends on the number of steps taken, relative to the total number, but not on the length of the list.

We want to point out that all the results presented so far, even if they were explicitly derived for permutation invariant states, hold for any instance of the Grover algorithm with one searched item, i.e.  $M = 1$ . Indeed, the general single searched item  $|X_1\rangle$  in the Grover algorithm can be achieved by local unitaries from the symmetric state  $|11\dots 1\rangle$ , without changing its entanglement content.

### 2.3.2 Two solutions

Let us now consider the case of two searched items (i.e.  $M = 2$ ). As an illustrative example we consider the case in which both  $|00\dots 0\rangle$  and  $|11\dots 1\rangle$  are solutions of the search problem, thus the state  $|X_1\rangle$  is a GHZ state composed of  $n$  qubits, and the state at each step of the computation is still permutation invariant. Thanks to permutation symmetry, the measure of any entanglement  $E_n$  is given by

$$\begin{aligned} E_n(|\psi_{k,M=2}\rangle) &= 1 - \max_{\alpha} \left| \frac{\cos \theta_k}{\sqrt{2^n - 2}} \left[ \left( \cos \frac{\alpha}{2} + \sin \frac{\alpha}{2} \right)^n \right. \right. \\ &\quad \left. \left. - \left( \cos^n \frac{\alpha}{2} + \sin^n \frac{\alpha}{2} \right) \right] + \frac{\sin \theta_k}{\sqrt{2}} \left( \cos^n \frac{\alpha}{2} + \sin^n \frac{\alpha}{2} \right) \right|^2. \end{aligned} \quad (2.14)$$

We maximized this quantity numerically; in Fig. 2.5 we show the behaviour for  $n = 13$ . Notice that after  $k_{opt}$  iterations, the measure  $E_n(|\psi_{k,M=2}\rangle)$  is no longer zero but equal to  $1/2$ . That is because the final state is no longer fully separable but instead it is close to the GHZ state. In this case the maximal value that the entanglement reaches during the computation is about  $2/3$ , i.e. higher than the case  $M = 1$ . Furthermore, this maximum is no longer reached at half of the optimal number of steps  $k_{opt}$ , but in a later step, i.e.  $k/k_{opt} \simeq 0.61$ .

Regarding genuine multipartite entanglement,  $E_2$  with two symmetric solutions can be computed by following an analogous procedure as for a single

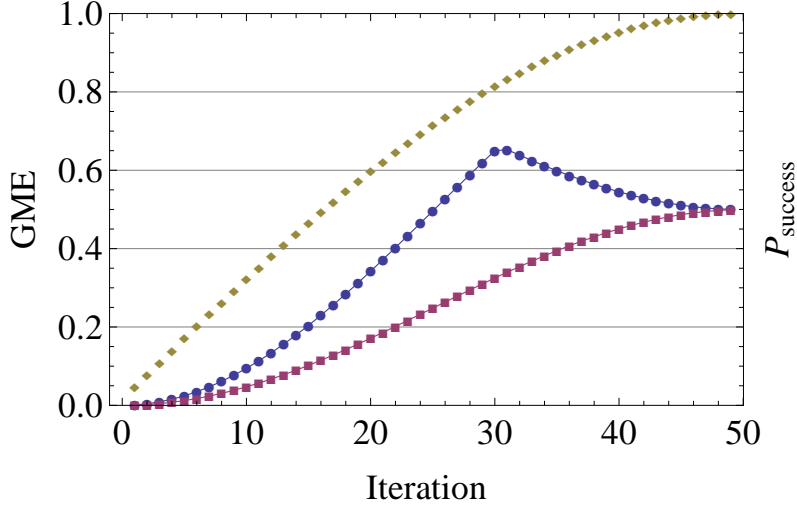


Figure 2.5: The GME as a function of the number of steps  $k$ , for two symmetric solutions of the search problem. The number of qubits is  $n = 13$ , and  $k_{opt} = 49$ .  $E_n(|\psi_{k,M=2}\rangle)$  is given by blue dots,  $E_2(|\psi_{k,M=2}\rangle)$  by purple squares. The yellow dots represent the success probability.

solution. The reduced density matrix for the general bipartite splitting  $P|Q$ , where  $m$  qubits are in  $P$  and  $n - m$  in  $Q$ , is now given by

$$\rho_P = \begin{pmatrix} c & b & \dots & b & d \\ b & a & \dots & a & b \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b & a & \dots & a & b \\ d & b & \dots & b & c \end{pmatrix}, \quad (2.15)$$

where  $a, b, c$  are given below Eq. (2.10),  $d = a - 2A(A - B)$ , with now  $A = \cos \theta_k / \sqrt{2^n - 2}$  and  $B = \sin \theta_k / \sqrt{2}$ . It turns out (see appendix B.1) that again the maximum eigenvalue corresponds to the bipartite splitting with  $m = 1$ , and  $E_2(|\psi_{k,M=2}\rangle)$  can be expressed analytically as

$$E_2(|\psi_{k,M=2}\rangle) = 1 - \frac{2^n - 4}{2^n - 2} \cos^2 \theta_k - \left( \frac{\cos \theta_k}{\sqrt{2^n - 2}} + \frac{\sin \theta_k}{\sqrt{2}} \right)^2. \quad (2.16)$$

This result is shown in Fig. 2.5. Notice that multipartite entanglement has a different behaviour from  $E_n(|\psi_{k,M=2}\rangle)$ . It is a monotonically increasing function that approaches the maximum value of  $1/2$  when the computation stops.

In the asymptotic limit  $2^n \gg 1$  the GME can be expressed (see appendix

B.2) as

$$\begin{aligned} E_n(|\psi_{k,M=2}\rangle) &\simeq \begin{cases} \sin^2 \theta_k & \text{for } \theta_k \leq \arccos 1/\sqrt{3}, \\ \frac{1+\cos^2 \theta_k}{2} & \text{for } \theta_k > \arccos 1/\sqrt{3}, \end{cases} \\ E_2(|\psi_{k,M=2}\rangle) &\simeq \frac{1}{2} \sin^2 \theta_k. \end{aligned} \quad (2.17)$$

As a consequence, both quantities exhibit the same scale invariance behaviour as discussed above for the case with one searched item.

Notice that the above results can be generalized to those search problems in which the two solutions are different in all digits, namely whenever the two solutions have maximal Hamming distance  $d = n$ , but not to all search problems with  $M = 2$ .

## 2.4 Entanglement dynamics in the fixed-point $\pi/3$ quantum search algorithm

In the previous section we have shown that the amount of entanglement is non-vanishing during the Grover algorithm and that its behaviour is scale invariant for a single solution to the search problem and in some instances of two solutions. We now show that a similar entanglement dynamics can be found in the fixed-point  $\pi/3$  quantum search. This kind of quantum search algorithm was first introduced in [49] to overcome the fact that the Grover algorithm might lead to a high error probability if the number of solutions  $M$  is unknown, since it requires to stop at a precise iteration  $k_{opt}$ , which depends on  $M$ . In contrast, the  $\pi/3$  quantum search always converges to the solutions, and thus it can be regarded as a fixed-point algorithm, even if it is never as fast as the standard Grover algorithm.

A possible way to realize such a fixed-point search is to slightly modify the operations  $U_f$  and  $\mathcal{I}$ , introduced in Sec. 2.1, in order to produce a  $\pi/3$  shift instead of a  $\pi$  shift [49], i.e.

$$\begin{aligned} U_f &\longrightarrow U_{\frac{\pi}{3}} = \mathbb{1} - (1 - e^{i\frac{\pi}{3}}) |X_1\rangle \langle X_1|, \\ \mathcal{I} &\longrightarrow \mathcal{I}_{\frac{\pi}{3}} = -(\mathbb{1} - (1 - e^{i\frac{\pi}{3}}) |\psi_0\rangle \langle \psi_0|). \end{aligned} \quad (2.18)$$

Then, the sequence of gates to be applied is defined by the following recursive formula

$$\begin{aligned} A_{m+1} &= A_m \mathcal{I}_{\frac{\pi}{3}} A_m^\dagger U_{\frac{\pi}{3}} A_m, \\ A_0 &= \mathbb{1}. \end{aligned} \quad (2.19)$$

We now compute both  $E_n$  and  $E_2$  for the employed states at each recursive step  $m$  of the evolution. The results were obtained numerically and are shown in Figs. 2.6 and 2.7 for both one and two solutions. Notice that the entangle-

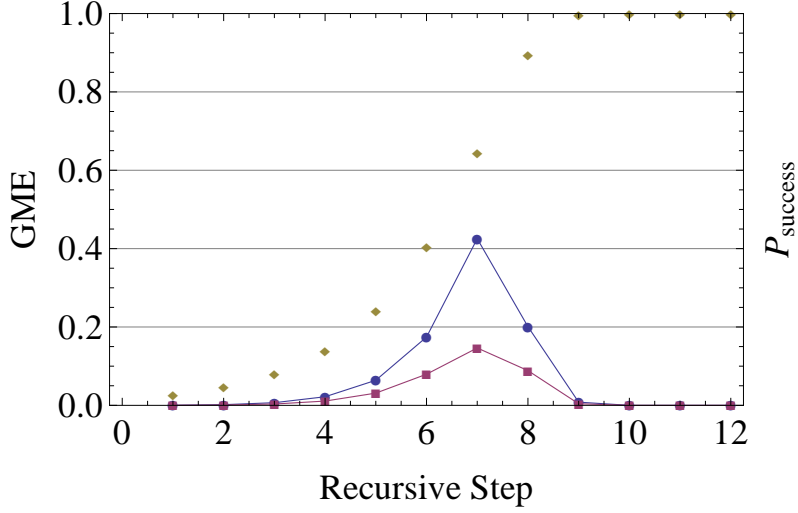


Figure 2.6: Evolution of entanglement in the  $\pi/3$  search as a function of the recursive step  $m$ , for a single searched item, with  $n = 12$  qubits. Here and in the following Fig. 2.7 blue dots, purple squares and yellow dots denote  $E_n$ ,  $E_2$  and the success probability, respectively.

ment behaviour of both  $E_n$  and  $E_2$  is similar to the dynamics of the standard Grover algorithm. These results indicate that entanglement plays the same crucial role in both algorithms, even if a scale invariance property cannot be proved in the fixed-point algorithm case.

## 2.5 Classical simulatability of Grover's algorithm

As a final comment, we may wonder whether the presence of true multipartite entanglement means that Grover's algorithm cannot be simulated efficiently by classical means. By efficient classical simulation of Grover's algorithm we mean that, given a database of  $n$  qubits, i.e.  $2^n$  items, it is possible to classically simulate Grover's algorithm with a total cost that scales as  $\sqrt{2^n} \text{poly}(n)$ . In this section we show that well-known criteria which guarantee efficient simulatability do not apply for Grover's algorithm.

According to the Gottesman-Knill theorem [1, 11], if a quantum computation starts in a computational basis state and involves only stabilizer gates (i.e. Hadamard, CNOT, phase gates and measurement of operators in the Pauli group), then it can be efficiently simulated on a classical computer. However, it is easy to shown that

$$\mathcal{I}(\sigma_z \otimes \mathbb{1}^{(n-1)})\mathcal{I}^\dagger = -\sigma_z \otimes \mathcal{I}^{(n-1)}. \quad (2.20)$$

Namely,  $\mathcal{I}$  defined in Sec. 2.1 turns an element belonging to the Pauli group,

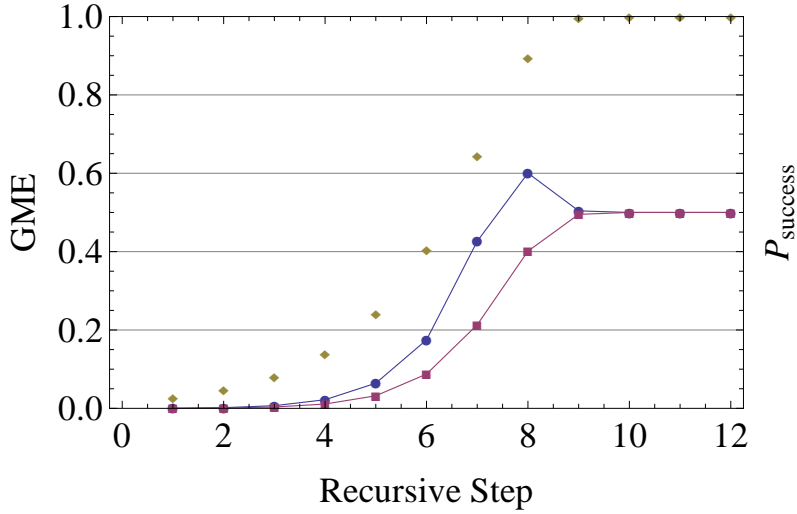


Figure 2.7: Evolution of entanglement in the  $\pi/3$  search as a function of the recursive step  $m$ , for two symmetric solutions of the search problem, with  $n = 13$  qubits.

i.e.  $\sigma_z \otimes \mathbb{1}^{(n-1)}$ , into an operator that no longer belongs to the Pauli group (here  $\mathcal{I}^{(n-1)}$  represents the inversion about the mean operator acting on  $n - 1$  qubits, instead of  $n$ ). Therefore,  $\mathcal{I}$  cannot be implemented by stabilizer gates, and so the Grover iteration does not fit into the hypotheses of Gottesman-Knill theorem.

Let us also consider the simulatability criterion involving matrix product states (MPS) [50], and based on the maximal Schmidt rank  $\chi$  of  $|\psi\rangle$  over all possible bipartitions. According to [50], if  $\chi$  does not exceed  $\text{poly}(n)$  in a computation that consists of  $\text{poly}(n)$  elementary gates (i.e. one- and two-qubit gates) acting on pure states, then the computation can be classically simulated efficiently. We notice that for states of the form (2.2),  $\chi$  is upper bounded by  $M + 1$ . However, although there exists a decomposition of the Grover operation  $G$  into  $\text{poly}(n)$  elementary gates [1, 51], the state after the action of each two-qubit gate does not have a simple symmetric form and we no longer can keep track of the maximal Schmidt rank. Therefore, we cannot conclude efficient simulatability.

The last approach that we show in order to study classical simulatability is to investigate how much tangled the quantum circuit involved in Grover's algorithm is. Indeed it turns out [52] that there exists a clear connection between the explicit realization of the circuit and the applicability of two well-known simulatability criteria, namely simulation by using either MPS explained above or contracting tensor networks (CTN) [53]. In more details the result is found in Ref. [52] states as follows. Given a quantum circuit of  $n$  qubits and with only one- and two-qubit gates, for each qubit wire  $i$  let  $D_i$  be the number of two-qubit gates that touch or cross the wire  $i$ . Let  $D = \max_i D_i$ , i.e. the max-

imum number of two-qubit gates which touch or cross each wire in the circuit. If  $D$  scales logarithmically in  $n$ , i.e.  $D = O(\log n)$ , then the quantum computation can be efficiently simulated by applying either MPS or CTN. Let us move to the Grover algorithm and check whether this criterion can be applied in this particular case. Just for the sake of simplicity, let us focus on a single step of the Grover procedure. It is then easy to see that both the oracle  $U_f$  and the inversion about mean operation  $\mathcal{I}$  can be seen as  $n - 1$ -controlled phase gate. Therefore, we can implement them by adding an extra register of  $n - 2$  qubits and using  $2(n - 2)$  Toffoli gates [1, 51]. As a result, since each Toffoli gate involves a fixed number of CNOT gates, during each step of the Grover procedure the maximum number of gates touching or crossing each wire scales linearly in  $n$ ,  $D = O(n)$ , and thus also the Jozsa's argument turns out to be vane.

The above results show that, although the Grover operation cannot be implemented by stabilizer gates and therefore the Knill-Gottesman theorem cannot be applied, the employed states at each Grover iteration are only slightly entangled according to the criterion suggested in [50]. However, the circuitual structure needed to implement the Grover algorithm in terms of two-qubit gates turns out to be enough complicated not to apply the criterion stated in [52]. We would like to stress that, even though these insights point in the direction of a negative answer to the question of efficient simulatability of the present algorithm, they are nevertheless not sufficient to draw any certain conclusion about classical simulatability of Grover's algorithm.

## 2.6 Conclusions and comments

In this chapter we have exhaustively studied and quantified via the GME the amount of entanglement, both bipartite and multipartite, that the states employed in the Grover search algorithm typically show.

Firstly we have explicitly calculated the entanglement content that the Grover states show in the initial step, namely after the first oracle call. The entanglement content of these states turns out to vanish exponentially fast as the number of qubits composing the register increases. Furthermore, in the search for two items, the Hamming distance is found to play a role with respect to the entanglement content. Actually, for fixed number of qubits in the register, the state turns out to be more entangled for increasing Hamming distance.

Then, we have studied the evolution of entanglement in the whole Grover's algorithm. In particular, we have given an explicit formula for the amount of genuine multipartite entanglement, which is proved to be always non-zero throughout the computation. Interestingly, the dynamics of entanglement shows the behaviour of scale invariance, i.e. counter-intuitively the amount of entanglement employed in the algorithm does not depend on the length of the searched list, but only on the number of steps taken, relative to the optimal



## 2. Entanglement in Grover's Algorithm

---

number of steps. This feature allows us to identify a unique entanglement dynamics, fixed a small number of solutions  $M = 1, 2$ , independently of the size of the register on which the search is performed. The entanglement evolution can thus be regarded as a property of the search problem under consideration, rather than of the quantum states employed in the computation. Since scale invariance is an important phenomenon in several areas of physics and mathematics, our results may open new avenues in the understanding of scale invariance properties of entanglement in other contexts, such as for example in many-body systems and phase transitions.

We have also compared the dynamics of entanglement in the standard Grover algorithm with the dynamics of entanglement shown by a different kind of search algorithm, i.e. the  $\pi/3$  quantum search, and we have proved that the entanglement content exhibits a similar behaviour.

At last we have tried to answer the question concerning whether the presence of true multipartite entanglement means that Grover's algorithm cannot be simulated efficiently by classical means. We have found that well-known criteria which guarantee efficient simulatability do not apply for Grover's algorithm, thus the question of simulatability of the Grover algorithm still remains open.

# Chapter 3

## Quantum Channel Detection

The possibility of determining properties of quantum communication channels or quantum devices is of great importance in order to be able to design and operate the channel at the best of its performances. In many realistic implementations some a priori information on the form of a quantum channel, or a quantum noise process, is available and it is of great interest to determine experimentally whether the channel has a certain property, by avoiding full quantum process tomography, which allows a complete reconstruction of the channel but it requires a large number of measurement settings [1].

In this chapter we present an efficient method to detect properties of quantum channels, assuming that some a priori information about the form of the channel is available [22, 23, 28]. The method relies on a correspondence with entanglement detection methods for multipartite density matrices based on witness operators. We first illustrate the method in the case of entanglement breaking channels and non separable random unitary channels, and show how it can be implemented experimentally by means of local measurements. We then study the detection of non separable maps and show that for pairs of systems of dimension higher than two the detection operators are not the same as in the random unitary case, highlighting a richer separability structure of quantum channels with respect to quantum states. Finally we consider the important sets of either PPT channel, completely co-positive channels, and bi-entangling operations, developing some techniques to reveal maps outside each of these sets.

### 3.1 Main idea and mathematical tools

By quantum channel detection (QCD) we mean the detection of a particular property of a quantum channel without performing the full quantum tomography of the process. Roughly speaking, the idea of QCD comes from the application of the entanglement witness (EW) formalism for revealing entangled states to quantum channels. The key ingredient is then the convexity of

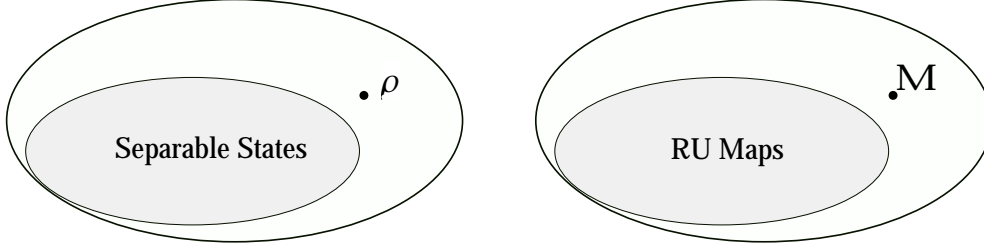


Figure 3.1: Comparison between the sets of quantum states and quantum maps. The set of random unitary channels is denoted by RU, and it is defined in Eq. (3.17).

the set we want to detect (as e.g. random unitary (RU) maps), as will be clear later.

For instance, just to clarify things, an EW acting on two qubits separates the convex subset of separable states from the set of entangled states we want to detect. In the same fashion, we can imagine a sort of map (we will give a more precise definition and a coherent interpretation later) which cuts the set of all quantum channels dividing the set of RU maps from the to-be-detected map. Figure 3.1 explains quite well this idea: to separate the non-RU map  $\mathcal{M}$  (in the EW formalism this would correspond to the entangled state  $\rho$ ) from the set of RUs (corresponding to the set of separable states). This straightforward comparison allows us to think about many similarities between EW and QCD, however we have to be careful not to push this reasoning too further, since there are many crucial differences between QCD and EW (as e.g. the subset of separable states still spans the whole set of states while the subset of RUs no longer does it).

The QCD method is mainly based on two ingredients: the concept of witness operators for entangled states [20] and the Choi-Jamiołkowski isomorphism [54, 55], which will be developed in the following.

#### 3.1.1 Entanglement detection

An hermitian operator  $W$  is called an EW for the entangled state  $\rho_{ent}$  if and only if the following inequalities hold

$$\begin{aligned} \text{Tr}[W\rho_{sep}] &\geq 0 \text{ for all separable states } \rho_{sep}, \\ \text{Tr}[W\rho_{ent}] &< 0 \text{ for at least the entangled state } \rho_{ent}. \end{aligned} \quad (3.1)$$

Thus, by definition,  $W$  is always a positive-semidefinite operator if restricted to the set of separable states. As a consequence, the states with negative expectation value, i.e.  $\text{Tr}[W\rho_{ent}] < 0$ , must be entangled. We say that these states are detected by the witness  $W$ . The essential ingredient that allows us to construct such an operator is actually the convexity of the subset of separable states. Indeed, due to the linearity of the trace, the states  $\rho$  fulfilling

$\text{Tr}[W\rho] = 0$  lie on a hyperplane which cuts the set of all states in two parts. The convexity is thus needed to guarantee that all separable states  $\rho_{sep}$  lie in the part with  $\text{Tr}[W\rho_{sep}] \geq 0$ , while the entangled states detected by  $W$  lie in the part where  $\text{Tr}[W\rho_{ent}] < 0$  holds. There are several ways to construct the operator  $W$ , however we will mainly focus on witness operators based on the geometric measure of entanglement (GME) [48, 56]. This choice is made essentially in the light of the further generalization to QCD.

Assume we are given an entangled pure state  $|\psi\rangle$  of a bipartite system. Therefore, a witness  $W$  detecting entanglement “around” this state can be constructed as

$$W = \alpha^2 \mathbb{1} - |\psi\rangle\langle\psi|, \quad (3.2)$$

where the coefficient  $\alpha^2$  is the squared overlap between the closest separable state  $|\phi\rangle \in S_2$  and the entangled state  $|\psi\rangle$ , in formulae

$$\alpha^2 = \max_{|\phi\rangle \in S_2} |\langle\psi|\phi\rangle|^2. \quad (3.3)$$

This construction deeply relies on the GME  $E_2$  defined in Eq. (2.3), as it is clear from the fact that  $\text{Tr}[W|\psi\rangle\langle\psi|] = \alpha^2 - 1 = -E_2(|\psi\rangle)$ . Notice that, since the maximum of a linear function over a convex set is always achieved on the extremal points, the maximum above can be always calculated by maximizing over pure separable states. Furthermore, it is easy to prove that the  $\alpha$  above is the smallest coefficient leading to either the largest negativity of  $W$  for  $|\psi\rangle$  and a positive expectation value over all separable states. Thus,  $W$  is clearly optimal among the witnesses of this form.

### 3.1.2 Quantum channels and the Choi-Jamiołkowski isomorphism

We firstly recall the reader that quantum channels, and in general quantum noise processes, are described by completely positive (CP) and trace preserving (TP) maps  $\mathcal{M}$ , which can be expressed in the Kraus form [19] as

$$\mathcal{M}[\rho] = \sum_k A_k \rho A_k^\dagger, \quad (3.4)$$

where  $\rho$  is the density operator of the quantum system on which the channel acts and the Kraus operators  $\{A_k\}$  fulfil the TP constraint  $\sum_k A_k^\dagger A_k = \mathbb{1}$ .

The detection method proposed is based on the Choi-Jamiołkowski isomorphism [54, 55], which gives a one-to-one correspondence between CP-TP maps acting on  $\mathcal{D}(\mathcal{H})$  (the set of density operators on  $\mathcal{H}$ , with arbitrary finite dimension  $d$ ) and bipartite density operators  $C_{\mathcal{M}}$  on  $\mathcal{H} \otimes \mathcal{H}$  with  $\text{Tr}_A[C_{\mathcal{M}}] = \mathbb{1}_B$ . This isomorphism can be described as:

$$\mathcal{M} \Longleftrightarrow C_{\mathcal{M}} = (\mathcal{M} \otimes \mathcal{I})[|\alpha\rangle\langle\alpha|], \quad (3.5)$$

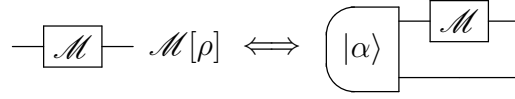


Figure 3.2: Scheme showing the Choi-Jamiołkowski isomorphism: on the left the map  $\mathcal{M}$ , on the right the corresponding Choi state  $C_{\mathcal{M}}$ .

where  $\mathcal{I}$  is the identity map, and  $|\alpha\rangle$  is the maximally entangled state with respect to the bipartite space  $\mathcal{H} \otimes \mathcal{H}$ , i.e.  $|\alpha\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^d |k\rangle |k\rangle$ . This is schematically depicted in Fig. 3.2. Notice that in the Kraus description the Choi state  $C_{\mathcal{M}}$  corresponding to the map  $\mathcal{M}$  takes the form

$$C_{\mathcal{M}} = \sum_k (A_k \otimes \mathbb{1}) |\alpha\rangle \langle \alpha| (A_k^\dagger \otimes \mathbb{1}) . \quad (3.6)$$

A fruitful approach is then to think of a specific subset of quantum channels in terms of the corresponding bipartite states. We thus reduce the problem of detecting the map  $\mathcal{M}$  to the already known problem of detecting the Choi state  $C_{\mathcal{M}}$ . This obviously comes at a cost, the dimension of the state to be revealed increases, since it now belongs to  $\mathcal{H} \otimes \mathcal{H}$ , instead of  $\mathcal{H}$ . Notice that in general we can find a connection between the set of maps we want to rule out and the entanglement class of the corresponding Choi states. This concept will be developed and clarified in the following sections.

## 3.2 Entanglement breaking channels

In this section we clarify the main idea of the proposed quantum channel detection method by considering as a first simple case the class of entanglement breaking (EB) channels [24]. A possible definition for an EB channel is based on the separability of its Choi state: a quantum channel is EB if and only if its Choi state is separable. This allows us to formulate a method to detect whether a quantum channel is not EB by exploiting entanglement detection methods designed for bipartite systems [57].

As a simple example of quantum channel detection consider the case of qubits and the single-qubit depolarising channel, defined as

$$\Gamma_p[\rho] = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i, \quad (3.7)$$

where  $\sigma_0$  is the identity operator,  $\{\sigma_i\}$  ( $i = 1, 2, 3$ ) are the three Pauli operators  $\sigma_x, \sigma_y, \sigma_z$  respectively (for brevity of notation in the following the Pauli operators will be denoted by  $X, Y$  and  $Z$ ), and  $p_0 = 1 - p$  (with  $p \in [0, 1]$ ), while  $p_i = p/3$  for  $i = 1, 2, 3$ . Such a channel is EB for  $p \geq 1/2$ . The corresponding set of Choi bipartite density operators is given by the Werner states

$$C_{\Gamma_p} = (1 - \frac{4}{3}p) |\alpha\rangle \langle \alpha| + \frac{p}{3} \mathbb{1} . \quad (3.8)$$

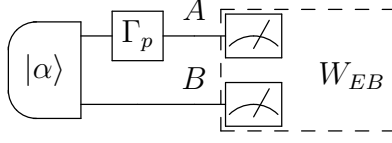


Figure 3.3: Experimental scheme showing the detection of the depolarising channel  $\Gamma_p$  as a non EB channel. The expectation value of  $W_{EB}$  is measured locally.

It is then possible to detect whether a depolarising channel is not EB by exploiting a detection operator suitable for the above set of states [57, 58], namely

$$W_{EB} = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} - X \otimes X + Y \otimes Y - Z \otimes Z). \quad (3.9)$$

The method can then be experimentally implemented by preparing a two-qubit state in the maximally entangled state  $|\alpha\rangle$ , then operating with the quantum channel to be detected on one of the two qubits and measuring the operator  $W_{EB}$  acting on both qubits at the end (see Fig. 3.3). If the resulting average value of  $W_{EB}$  is negative, we can then conclude that the channel  $\Gamma_p$  under consideration is not EB. Notice that the final measurement can be performed locally by decomposing  $W_{EB}$  into local operators (see Eq. (3.9)).

We now show that our method provides also a lower bound on a particular feature of EB channels recently defined in Ref. [59] as follows. Let  $\mathcal{M}$  be a generic map acting on a qudit (i.e. a  $d$ -dimensional system) and  $\mathcal{D}_\sigma$  the completely depolarizing channel defined as  $\mathcal{D}_\sigma[\rho] = \sigma$ , where  $\sigma$  is an arbitrary state. The quantity  $\mu_c(\mathcal{M})$  is defined as the minimum value of the mixing probability parameter  $\mu \in [0, 1]$  that transforms the convex combination  $(1 - \mu)\mathcal{M} + \mu\mathcal{D}_\sigma$  into an EB channel, i.e. in formulae

$$\mu_c(\mathcal{M}) = \min_{\sigma} \{ \mu | (1 - \mu)\mathcal{M} + \mu\mathcal{D}_\sigma \in \text{EB} \}. \quad (3.10)$$

Clearly  $\mu_c(\mathcal{M})$  nullifies if  $\mathcal{M}$  is already an EB channel. By the Choi-Jamiołkowski isomorphism, we can rephrase the definition (3.10) in term of Choi states as

$$\mu_c(\mathcal{M}) = \min_{\sigma} \left\{ \mu | (1 - \mu)C_{\mathcal{M}} + \mu\sigma \otimes \frac{\mathbb{1}}{d} \in \text{Sep} \right\}, \quad (3.11)$$

and link this quantity to the well-known generalized robustness of entanglement.

Given a state  $\rho$ , the generalized robustness of entanglement is defined [60, 61] as the minimal  $s > 0$  such that the state  $\frac{\rho + s\sigma}{1+s}$  is separable, where  $\sigma$  is an arbitrary state (not necessarily separable), namely

$$R(\rho) = \min_{\sigma} \{ s | \frac{\rho + s\sigma}{1+s} \in \text{Sep} \}. \quad (3.12)$$

This quantity can be interpreted as the minimum amount of noise necessary to wash out completely the entanglement initially present in the state  $\rho$ . Thus,

### 3. Quantum Channel Detection

---

by defining  $p_c(\rho) = 1 - \frac{1}{1+R(\rho)}$  and interpreting  $\rho$  as the Choi state  $C_{\mathcal{M}}$  corresponding to the map  $\mathcal{M}$ , we can bound  $\mu_c(\mathcal{M})$  as

$$\mu_c(\mathcal{M}) \geq p_c(C_{\mathcal{M}}). \quad (3.13)$$

This can be seen from Eq. (3.12), since the minimizing set involved in the definition (3.11) of  $\mu_c(\mathcal{M})$  is smaller than the minimizing set considered for  $R(\rho)$ . We can then derive a bound for the generalized robustness from the experimental data of an entanglement detection procedure [62] as

$$R(\rho) \geq |c|/w_{\max}, \quad (3.14)$$

where  $c$  is measured experimentally via the expectation value of the witness, i.e.  $\text{Tr}[W\rho] = c < 0$ , while  $w_{\max}$  is the maximal eigenvalue of the operator  $W$ . As a result, we find that

$$\mu_c(\mathcal{M}) \geq 1 - \frac{1}{1 + |c|/w_{\max}}, \quad (3.15)$$

which links the expectation value  $c$  measured experimentally with the theoretical quantity  $\mu_c(\mathcal{M})$ .

In the case of the depolarising channel (3.7) with  $p < 1/2$ , by using the detection operator  $W_{EB}$  given by Eq. (3.9) (with  $c = p - 1/2$  and  $w_{\max} = 1/2$ ), the above bound takes the form

$$\mu_c(\Gamma_p) \geq \frac{1 - 2p}{2 - 2p}. \quad (3.16)$$

In this case, however, the bound turns out to be not tight since the theoretical  $\mu_c(\Gamma_p)$  can be computed to be  $\frac{2-4p}{3-4p}$  by following the method developed in [59].

### 3.3 Separable random unitaries

We now consider the case of RU channels, defined as

$$\mathcal{U}[\rho] = \sum_k p_k U_k \rho U_k^\dagger, \quad (3.17)$$

where  $U_k$  are unitary operators and  $p_k > 0$  with  $\sum_k p_k = 1$ . Notice that this kind of maps includes several interesting models of quantum noisy channels, such as the already mentioned depolarising channel or the phase damping channel and the bit flip channel [1]. RUs were also studied extensively and characterised in Ref. [63].

We now consider the case where the RU channel acts on a bipartite system  $AB$  as follows

$$\mathcal{V}[\rho_{AB}] = \sum_k p_k (V_{k,A} \otimes W_{k,B}) \rho_{AB} (V_{k,A}^\dagger \otimes W_{k,B}^\dagger), \quad (3.18)$$

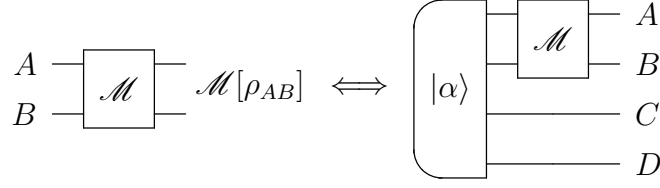


Figure 3.4: Scheme of the Choi-Jamiołkowski isomorphism in the case of four-partite states. The state  $|\alpha\rangle$  on the right is the maximally entangled state with respect to the bipartition  $AB|CD$ .

where both  $V_{k,A}$  and  $W_{k,B}$  are unitary operators for all  $k$ 's, acting on systems  $A$  and  $B$ , respectively. Quantum channels of the above form are named separable random unitaries (SRUs) and they form a convex subset in the set of all CP-TP maps acting on bipartite systems. Interesting examples of channels of this form are given by Pauli memory channels [64].

The Choi state corresponding to quantum channels acting on bipartite systems is a four-partite state (composed of systems  $A, B, C$  and  $D$ ), as shown in Fig. 3.4. Notice that the state  $|\alpha\rangle = \frac{1}{\sqrt{d_{AB}}} \sum_{k,j=1}^{d_{AB}} |k,j\rangle_{AB} |k,j\rangle_{CD}$  (where  $d_{AB} = d_A d_B$  is now the dimension of the Hilbert space of the bipartite system  $AB$ ) can also be written as  $|\alpha\rangle = |\alpha\rangle_{AC} |\alpha\rangle_{BD}$ , namely it is a biseparable state for the partition  $AC|BD$  of the global four-partite system. The Choi states corresponding to SRU channels therefore form a convex set, which is a subset of all biseparable states for the partition  $AC|BD$ . Since the generating set of SRUs is given by local unitaries  $U_A \otimes U_B$ , the generating biseparable pure states in the corresponding set of Choi states have the form

$$|U_A \otimes U_B\rangle = (U_A \otimes \mathbb{1}_C) |\alpha\rangle_{AC} \otimes (U_B \otimes \mathbb{1}_D) |\alpha\rangle_{BD} . \quad (3.19)$$

We name the set of four-partite Choi states corresponding to SRUs as  $S_{SRU}$ . It is now possible to design detection procedures for SRU maps by employing suitable operators that detect the corresponding Choi state with respect to biseparable states (in  $AC|BD$ ) belonging to  $S_{SRU}$ .

We now focus on the case of a unitary transformation  $U$  acting on two qudits, that is explicitly supposed to be non separable. The corresponding Choi state is pure and has the form

$$|U\rangle = (U \otimes \mathbb{1}) |\alpha\rangle . \quad (3.20)$$

Therefore, in the same spirit as for the witness of Eq. (3.2), a suitable detection operator for  $U$  as a non SRU gate can be constructed as

$$W_{SRU} = \alpha_{SRU}^2 \mathbb{1} - C_U , \quad (3.21)$$

where  $C_U = |U\rangle \langle U|$ , and the coefficient  $\alpha_{SRU}$  is the overlap between the closest biseparable state in the set  $S_{SRU}$  and the entangled state  $|U\rangle$ , namely

$$\alpha_{SRU}^2 = \max_{\mathcal{M}_{SRU}} \langle U | C_{\mathcal{M}_{SRU}} | U \rangle . \quad (3.22)$$



### 3. Quantum Channel Detection

---

Notice that, since the maximum of a linear function over a convex set is always achieved on the extremal points, the maximum above can be calculated by maximizing over the pure biseparable states (3.19), i.e.

$$\alpha_{SRU} = \max_{U_A, U_B} |\langle U_A \otimes U_B | U \rangle| = \frac{1}{d^2} \max_{U_A, U_B} |\text{Tr}[(U_A^\dagger \otimes U_B^\dagger)U]|. \quad (3.23)$$

Recall that the Choi states given by Eq. (3.19) correspond to the generating points for SRU channels, which is actually a superset of the extremal points of the SRU set.

As an example of the above procedure consider the CNOT gate acting on a two-qubit system, defined by

$$\text{CNOT} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & X \end{pmatrix}, \quad (3.24)$$

with  $\mathbb{1}$  representing the  $2 \times 2$  identity matrix, and  $X$  the usual Pauli operator. The coefficient  $\alpha_{SRU}$  for  $U = \text{CNOT}$  can be computed as follows. The state of Eq. (3.20) specialized for the CNOT gate is clearly not separable with respect to the split  $AC|BD$  and it can be expressed in the Schmidt decomposition regarding that split as

$$|\text{CNOT}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AC} |\alpha\rangle_{BD} + |11\rangle_{AC} |\psi^+\rangle_{BD}), \quad (3.25)$$

where  $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ . The above expression naturally proves that the maximum overlap with any biseparable state with respect to  $AC|BD$  cannot exceed the value of  $1/\sqrt{2}$ . Since the convex set  $S_{SRU}$  of allowed states in our optimisation problem is smaller than the set of all biseparable states, this would provide only an upper bound for the maximum overlap  $\alpha_{SRU}$ . However, two local unitary operations  $U_A$  and  $U_B$  that saturate this bound can be explicitly found, namely

$$U_A = S, \quad (3.26)$$

$$U_B = e^{-i\frac{\pi}{4}X}, \quad (3.27)$$

where  $S$  is the phase gate given by  $S = \text{diag}(1, i)$ . This finally proves that the optimal coefficient  $\alpha_{SRU}$  equals  $1/\sqrt{2}$  even if we restrict to the set of biseparable states  $S_{SRU}$ . Moreover, the detection operator  $W_{\text{CNOT}} = \frac{1}{2}\mathbb{1} - C_{\text{CNOT}}$  can be decomposed into a linear combination of local operators as follows

$$\begin{aligned} W_{\text{CNOT}} = \frac{1}{64} & (3\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} - \mathbb{1}X\mathbb{1}X - XXX\mathbb{1} - X\mathbb{1}XX \\ & - ZZ\mathbb{1}Z + ZY\mathbb{1}Y + YYXZ + YZXY \\ & - Z\mathbb{1}Z\mathbb{1} - ZXZX + YXY\mathbb{1} + Y\mathbb{1}YX \\ & - \mathbb{1}ZZZ + \mathbb{1}YZY + XYYZ + XZYY), \end{aligned} \quad (3.28)$$

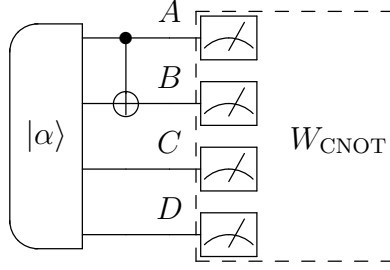


Figure 3.5: Experimental scheme implementing the detection of the CNOT gate as a non SRU map.

where for simplicity of notation the tensor product symbol has been omitted. As we can see from the above form, the CNOT can be detected by using nine different local measurements settings, namely  $\{XXXX, ZZZZ, ZYZY, YXYX, YYXZ, YZXY, ZXZX, XYYZ, XZYY\}$ . Actually, in the first line of the above expression the expectation values of operators  $\mathbb{1}X\mathbb{1}X, XXX\mathbb{1}, X\mathbb{1}XX$  can be obtained by measuring the operator  $XXXX$  and suitably processing the experimental data. Similar groupings can be done for the other terms in Eq. (3.28), such that the only measurement settings needed are the nine listed above. Following [57, 65], it can be also easily proved that the above form is optimal in the sense that it involves the smallest number of measurement settings. From an experimental point of view, the optimal detection procedure can be implemented as follows: prepare a four-qubit system in the state  $|\alpha\rangle = |\alpha\rangle_{AC} |\alpha\rangle_{BD}$ , apply the quantum channel to qubits  $A$  and  $B$ , and finally perform the set of nine local measurements reported above in order to measure the operator  $W_{\text{CNOT}}$  of (3.28). If the resulting average value is negative then the quantum channel is detected as a non SRU map. The experimental scheme is shown in Fig. 3.5. Notice that the number of measurements needed in this procedure is much smaller than the one required for complete quantum process tomography, since the former scales as  $d_{AB}^2$  [58, 66] while the latter as  $d_{AB}^4$  [1].

The number of measurement settings in the detection scheme can be further decreased if we allow a non optimal detection operator, in the sense that the coefficient  $\alpha_{\text{SRU}}$  in  $W_{\text{CNOT}}$  is smaller than the maximum value. In this case, since the state  $C_{\text{CNOT}}$  is a stabilizer state with generators  $\{XXX\mathbb{1}, \mathbb{1}X\mathbb{1}X, Z\mathbb{1}Z\mathbb{1}, ZZ\mathbb{1}Z\}$ , an alternative detection operator can be derived, following the approach of Ref. [37]. The resulting suboptimal detection operator turns out to be

$$\tilde{W}_{\text{CNOT}} = 3\mathbb{1} - 2 \left[ \frac{(\mathbb{1} + XXX\mathbb{1})(\mathbb{1} + \mathbb{1}X\mathbb{1}X)}{2} + \frac{(\mathbb{1} + Z\mathbb{1}Z\mathbb{1})(\mathbb{1} + ZZ\mathbb{1}Z)}{2} \right], \quad (3.29)$$

which requires only the two local measurement settings  $\{XXXX, ZZZZ\}$ .

The robustness of the method in the detection of the CNOT gate is extensively analysed in [28] and will be discussed in the next chapter.

## 3.4 Separable maps

We now focus on the detection of non separable maps. By definition, a separable map  $\mathcal{M}_{sep}$  is given by

$$\mathcal{M}_{sep}[\rho_{AB}] = \sum_k (A_k \otimes B_k) \rho_{AB} (A_k^\dagger \otimes B_k^\dagger), \quad (3.30)$$

namely it can be written in terms of separable Kraus operators [26]. In this section we do not require the TP constraint to be fulfilled. Notice that the set of separable maps is a larger set than the set of SRUs studied above. A general map  $\mathcal{M}$  acting on two qudits is not separable if and only if the corresponding Choi state  $C_{\mathcal{M}}$  is entangled with respect to the splitting  $AC|BD$  [25].

Analogously to the case of SRU maps, for a non separable unitary  $U$  we can define a detection operator of the same form of Eq. (3.21), i.e.

$$W_S = \alpha_S^2 \mathbb{1} - C_U, \quad (3.31)$$

where now the coefficient  $\alpha_{SRU}^2$  is replaced by  $\alpha_S^2$  defined as

$$\alpha_S^2 = \max_{\mathcal{M}_{sep}} \langle U | C_{\mathcal{M}_{sep}} | U \rangle. \quad (3.32)$$

Since the set of SRUs is a subset of all separable maps, in general  $\alpha_S \geq \alpha_{SRU}$  holds, see Fig 3.6. Since the extremal points of the set of separable maps are by construction maps with a single Kraus operator, the maximum in Eq. (3.32) is attained on pure states (see appendix C.1). We can thus compute the maximum on pure Choi states  $C_{\mathcal{M}_{sep}}$  corresponding to separable maps of the form  $\mathcal{M}_{sep} = A \otimes B$ . The calculation of  $\alpha_S$  can then be simplified as

$$\alpha_S = \max_{A,B} |\langle A \otimes B | U \rangle| = \frac{1}{d^2} \max_{A,B} |\text{Tr}[(A^\dagger \otimes B^\dagger)U]|. \quad (3.33)$$

Notice that now we do not require  $A \otimes B$  to be TP, otherwise both the operators  $A$  and  $B$  would be automatically unitary, as they act on a finite dimensional Hilbert space. Interestingly, we now show that for a general unitary  $U$  on two-qubit systems the two coefficients  $\alpha_{SRU}$  and  $\alpha_S$  coincide, while for higher dimension this is no longer the case.

We compute the coefficients by starting from the Schmidt decomposition of an operator  $O$  acting on two qudits, which can be written as

$$O = \sum_{i=1}^r \lambda_i A_i \otimes B_i, \quad (3.34)$$

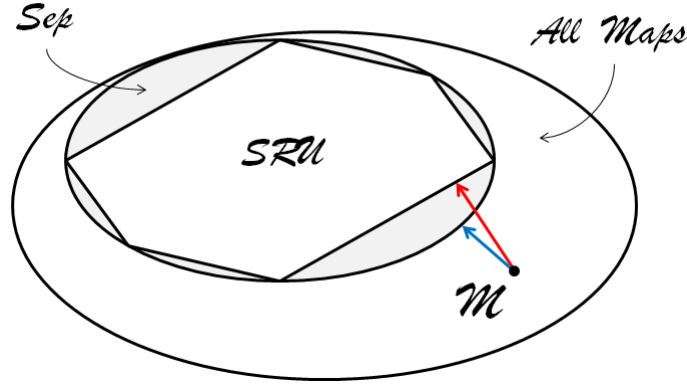


Figure 3.6: Pictorial scheme showing the relation  $\alpha_S \geq \alpha_{SRU}$ . Notice that the minimal distance between the map  $\mathcal{M}$  and the set of SRU channels (red), i.e.  $1 - \alpha_{SRU}^2$ , is achieved over the generating set of SRUs and is generally larger than the minimal distance with the set of separable maps (blue), i.e.  $1 - \alpha_S^2$ .

where  $\{A_i\}_{i=1,\dots,d^2}$  and  $\{B_i\}_{i=1,\dots,d^2}$  are two orthogonal bases ( $\text{Tr}[A_i^\dagger A_j] = \text{Tr}[B_i^\dagger B_j] = d\delta_{ij}$ ) for the operator space, and  $r$  is the Schmidt rank fulfilling  $1 \leq r \leq d^2$ . Notice that the unique Schmidt coefficients  $\lambda_i$  are always positive and ordered, i.e.  $\lambda_1 \geq \dots \geq \lambda_r$ . As a result, if we write the unitary  $U$  in the Schmidt decomposition (3.34), it follows that the maximum (3.33) is achieved by the choice of  $A \otimes B = A_1 \otimes B_1$ , where  $A_1$  and  $B_1$  are the operators corresponding to the largest Schmidt coefficient  $\lambda_1$ . We then have

$$\alpha_S = \frac{1}{d^2} |\text{Tr}[(A_1^\dagger \otimes B_1^\dagger)U]| = \lambda_1. \quad (3.35)$$

It is then interesting to establish whether the optimal separable operator  $A_1 \otimes B_1$  has to be unitary as well. As mentioned above, we will show in the following that this is true for two-qubit systems but no longer holds when the dimension increases. We first show that for two qubits it is always possible to find a separable unitary  $U_A \otimes U_B$  such that the overlap with  $U$  achieves the maximum  $\lambda_1$ , namely

$$\exists U_A, U_B \text{ s.t. } |\langle U_A \otimes U_B | U \rangle| = \alpha_{SRU} = \lambda_1. \quad (3.36)$$

This is a consequence of the Cartan decomposition [67, 68] of a general unitary  $U$  acting on two qubits. Indeed  $U$  can be rewritten as

$$U = (V_A \otimes V_B) \tilde{U} (W_A \otimes W_B), \quad (3.37)$$

where  $V_A, V_B, W_A$  and  $W_B$  are single-qubit unitaries and

$$\tilde{U} = e^{i(\theta_x X \otimes X + \theta_y Y \otimes Y + \theta_z Z \otimes Z)}. \quad (3.38)$$

Notice that, by the definitions  $c_\alpha = \cos \theta_\alpha$  and  $s_\alpha = \sin \theta_\alpha$ ,  $\tilde{U}$  takes the form

$$\begin{aligned} \tilde{U} = & (c_x c_y c_z + i s_x s_y s_z) \mathbb{1} \otimes \mathbb{1} + (c_x s_y s_z + i s_x c_y c_z) X \otimes X \\ & + (s_x c_y s_z + i c_x s_y c_z) Y \otimes Y + (s_x s_y c_z + i c_x c_y s_z) Z \otimes Z. \end{aligned} \quad (3.39)$$

### 3. Quantum Channel Detection

---

According to (3.37), it is then straightforward to see that the above form of  $\tilde{U}$  directly leads to the Schmidt decomposition of  $U$ . By defining

$$c_x c_y c_z + i s_x s_y s_z \equiv \rho_0 e^{i2\phi_0}, \quad (3.40)$$

$$c_x s_y s_z + i s_x c_y c_z \equiv \rho_1 e^{i2\phi_1}, \quad (3.41)$$

$$s_x c_y s_z + i c_x s_y c_z \equiv \rho_2 e^{i2\phi_2}, \quad (3.42)$$

$$s_x s_y c_z + i c_x c_y s_z \equiv \rho_3 e^{i2\phi_3}, \quad (3.43)$$

we can indeed rewrite  $\tilde{U}$  as

$$\begin{aligned} \tilde{U} = & \rho_0 e^{i\phi_0} \sigma_0 \otimes e^{i\phi_0} \sigma_0 + \rho_1 e^{i\phi_1} \sigma_1 \otimes e^{i\phi_1} \sigma_1 \\ & + \rho_2 e^{i\phi_2} \sigma_2 \otimes e^{i\phi_2} \sigma_2 + \rho_3 e^{i\phi_3} \sigma_3 \otimes e^{i\phi_3} \sigma_3, \end{aligned} \quad (3.44)$$

with the notation  $\sigma_0 = \mathbb{1}$ ,  $\sigma_1 = X$ ,  $\sigma_2 = Y$  and  $\sigma_3 = Z$ . We now notice that the magnitudes of the coefficients in front of the bipartite operators correspond to the Schmidt coefficients themselves and the phases can be reabsorbed into the Pauli operators without changing the orthogonality relations. Hence, by setting  $A_i \equiv V_A e^{i\phi_i} \sigma_i W_A$  for the system  $A$  and  $B_i \equiv V_B e^{i\phi_i} \sigma_i W_B$  for  $B$ , we arrive at the following Schmidt decomposition of  $U$ :

$$U = \sum_{i=1}^4 \rho_i A_i \otimes B_i. \quad (3.45)$$

Therefore, given a unitary  $U$  on two qubits, it is always possible to find a local unitary achieving the maximum  $\lambda_1$ , since there always exists a Schmidt decomposition of  $U$  involving only unitary operators as local basis. For higher dimensional systems the above argument does not hold. Actually, already in the two-qutrit case it may happen that the maximum (3.35) can be attained only by local non unitary operators. This means that the closest (under the criterion defined in Eq. (3.33)) separable map to a unitary  $U$  may be non unitary.

We now show an explicit example for a system of two qutrits given by the gate  $Z_3$  defined as

$$Z_3 = \text{diag}(1, 1, 1, 1, 1, 1, 1, 1, -1), \quad (3.46)$$

which is clearly unitary and not separable. We can rewrite  $Z_3$  in the Schmidt form with Schmidt rank  $r = 2$  as

$$Z_3 = \lambda_1 A_1 \otimes B_1 + \lambda_2 A_2 \otimes B_2, \quad (3.47)$$

where  $\lambda_{1,2} = \sqrt{\frac{1}{2}(9 \pm \sqrt{17})}/3$ , while the operators  $A_{1,2}$  and  $B_{1,2}$  are non unitary and can be written as

$$A_{1,2} = \frac{\sqrt{3}}{\sqrt{102 \pm 22\sqrt{17}}} \text{diag}(5 \pm \sqrt{17}, 5 \pm \sqrt{17}, 1 \pm \sqrt{17}), \quad (3.48)$$

$$B_{1,2} = \frac{\sqrt{3}}{\sqrt{646 \pm 150\sqrt{17}}} \text{diag}(11 \pm 3\sqrt{17}, 11 \pm 3\sqrt{17}, 9 \pm \sqrt{17}). \quad (3.49)$$

From the Schmidt decomposition it immediately follows that the value of the maximum overlap is given by  $\alpha_S = \lambda_1 = \sqrt{\frac{1}{2}(9 + \sqrt{17})}/3 \simeq 0.854$ , while the coefficient  $\alpha_{SRU}$  can be computed numerically, leading to  $\alpha_{SRU} \simeq 0.786$  (see appendix C.2). Hence, this finally proves that for the gate  $Z_3$  the maximum attained over SRUs is strictly smaller than the maximum achieved by separable maps,  $\alpha_{SRU} < \alpha_S$ .

We want to stress that our method is then suitable to detect the gap between separable and SRU maps, as long as  $d \geq 3$ , by the amount of violation of the expectation value of  $W_{SRU}$ . For instance, the unitary  $Z_3$  can be detected as a non SRU map by an operator of the following form

$$W_{Z_3} = \alpha_{SRU}^2 \mathbb{1} - C_{Z_3}, \quad (3.50)$$

where  $C_{Z_3} = |Z_3\rangle\langle Z_3|$  and  $\alpha_{SRU} \simeq 0.786$ . The expectation value of  $W_{Z_3}$  over the Choi state of the experimentally accessible map  $\mathcal{M}$  thus allows us to distinguish between non SRU and non separable maps. Actually,  $\mathcal{M}$  is detected to be non SRU if  $\text{Tr}[W_{Z_3}C_{\mathcal{M}}] < 0$ , and in addition we can say that  $\mathcal{M}$  is non separable if  $\text{Tr}[W_{Z_3}C_{\mathcal{M}}] < \alpha_{SRU}^2 - \alpha_S^2$ . Therefore, as it always happens with states, if we want to distinguish between any kind of entanglement and multipartite entanglement, a stronger violation of the positivity of  $\text{Tr}[W_{SRU}C_{\mathcal{M}}]$  makes our knowledge of  $\mathcal{M}$  more accurate. Notice that the above discrimination works perfectly for systems composed of two qudits, with  $d \geq 3$ , but no longer works when we reduce to a two-qubit system, since in this latter case our method cannot distinguish between separable and SRU maps any more.

Last but not least, as it is the case for witnesses based on the GME [69], the detection operator  $W_S$  developed to reveal the non separability of  $U$  and defined in Eq. (3.31) provides a lower bound for the gate fidelity  $F(U, \mathcal{M})$  [66], namely

$$F(U, \mathcal{M}) = \text{Tr}[C_U C_{\mathcal{M}}] \geq \alpha_S^2 - \text{Tr}[W_{SRU} C_{\mathcal{M}}]. \quad (3.51)$$

Notice that the same argument holds for the detection operator  $W_{SRU}$  defined in Eq. (3.21); however, as the negativity of  $W_S$  is a stronger requirement than the negativity of  $W_{SRU}$ , the expectation value of the detection operator  $W_S$  provides a higher value for the gate fidelity  $F(U, \mathcal{M})$ .

### 3.5 PPT channels

In this section we consider a larger set of quantum channels, namely PPT channels. A CP map  $\mathcal{M}$  acting on two qudits is positive partial transpose (PPT) if and only if the composite map  $\mathcal{M}_{\mathcal{T}} = \mathcal{T}_A \circ \mathcal{M} \circ \mathcal{T}_A$ , being  $\mathcal{T}_A$  the partial transposition map on the first system  $A$ , is CP [27, 70]. Since a map  $\mathcal{M}$  is CP if and only if the corresponding Choi operator  $C_{\mathcal{M}}$  is positive, we can restate the above definition as: a CP map  $\mathcal{M}$  is PPT if and only if the Choi

### 3. Quantum Channel Detection

---

operator  $C_{\mathcal{M}\mathcal{T}}$  related to the composite map  $\mathcal{M}\mathcal{T}$  is positive. Notice that the above definition is different from the one given, for instance, in Ref. [71].

By the above correspondence we develop a method to detect whether a map is non-positive partial transpose (NPT). We employ techniques already developed for the detection of entangled NPT states [72], namely we consider a detection operator of the following form

$$W_{\text{PPT}} = |\lambda_{-}\rangle \langle \lambda_{-}|^{\mathcal{T}_A}, \quad (3.52)$$

where  $|\lambda_{-}\rangle$  is the eigenvector of the Choi state  $C_{\mathcal{M}\mathcal{T}}$  corresponding to the most negative eigenvalue  $\lambda_{-}$  for the NPT map  $\mathcal{M}$ .

The expectation value of the above detection operator should now be measured for the Choi operator corresponding to the composite map  $\mathcal{M} \circ \mathcal{T}_A$ , since the partial transposition following  $\mathcal{M}$  is already taken into account in the form of the operator (3.52). Therefore, a crucial point of this approach is now related to the implementation of the map  $\mathcal{T}_A$ , which is non CP. A possible solution is to add noise to the map  $\mathcal{T}_A$  in order to make it CP [73]. Following the approach of Ref. [73] we consider the minimal amount of depolarising noise such that the following map

$$\tilde{\mathcal{T}}_A[\rho_{AB}] = (1 - p)\mathcal{T}_A[\rho_{AB}] + p\frac{\mathbb{1}_{AB}}{d^2} \quad (3.53)$$

is CP. This is given by  $p = d^3/(d^3 + 1)$  [73]. From an experimental point of view, we then consider the implementation of the map  $\tilde{\mathcal{T}}_A$  instead of the non-physical map  $\mathcal{T}_A$ , as shown in Fig. 3.7. This procedure leads to an extra contribution in the expectation value of the detection operator, related to the presence of the depolarized term in Eq. (3.53). The expectation value of  $W_{\text{PPT}}$  for the Choi state  $C_{\mathcal{M} \circ \tilde{\mathcal{T}}_A}$  related to the composite map  $\mathcal{M} \circ \tilde{\mathcal{T}}_A$  is thus given by

$$\begin{aligned} \text{Tr}[W_{\text{PPT}} C_{\mathcal{M} \circ \tilde{\mathcal{T}}_A}] &= \\ &= (1 - p) \langle \lambda_{-} | C_{\mathcal{M}\mathcal{T}} | \lambda_{-} \rangle + p \langle \lambda_{-} | \mathcal{M}\mathcal{T} \left[ \frac{\mathbb{1}_{AB}}{d^2} \right] \otimes \frac{\mathbb{1}_{CD}}{d^2} | \lambda_{-} \rangle \\ &= (1 - p) \lambda_{-} + p \langle \lambda_{-} | \mathcal{M}\mathcal{T} \left[ \frac{\mathbb{1}_{AB}}{d^2} \right] \otimes \frac{\mathbb{1}_{CD}}{d^2} | \lambda_{-} \rangle. \end{aligned} \quad (3.54)$$

Notice that the negative term  $\lambda_{-}$  comes from the NPT-ness of the map  $\mathcal{M}$ , while the other term is due to the implementation of  $\tilde{\mathcal{T}}_A$  in the proposed experimental procedure. The expression above clearly shows that the operator  $W_{\text{PPT}}$  can be regarded as a witness with respect to the set of PPT maps, as its expectation value is always non-negative on this set. Therefore, if the expectation value of the detection operator  $W_{\text{PPT}}$  is negative, the map  $\mathcal{M}$  is guaranteed to be NPT. Notice that the expectation value given by Eq. (3.54) usually depends on the to-be-detected map  $\mathcal{M}$ , and generally the requirement of the negativity of the expectation value of  $W_{\text{PPT}}$  is stronger than what one actually need to be sure that  $\mathcal{M}$  is NPT. Therefore, in order to find the optimal

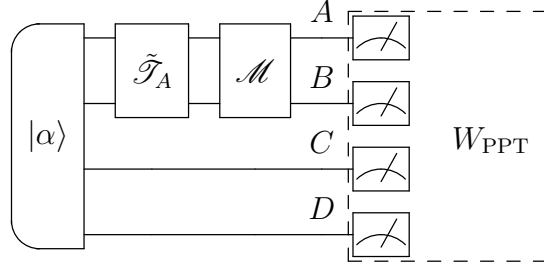


Figure 3.7: Experimentally-feasible scheme to implement the detection of the NPT map  $\mathcal{M}$ .

detection operator  $W_{\text{PPT}}$ , one should minimize the last term of Eq. (3.54) with respect to the set of all PPT maps  $\mathcal{M}^{\text{PPT}}$ , i.e.

$$\min_{\mathcal{M}^{\text{PPT}}} \langle \lambda_- | \mathcal{M}_{\mathcal{T}}^{\text{PPT}} \left[ \frac{\mathbb{1}_{AB}}{d^2} \right] \otimes \frac{\mathbb{1}_{CD}}{d^2} | \lambda_- \rangle, \quad (3.55)$$

a hard task that drastically simplifies when the map  $\mathcal{M}$  is promised to be unital.

Let us thus assume that the map  $\mathcal{M}$  is unital. The expectation value in Eq. (3.54) then takes the simple form

$$\text{Tr}[W_{\text{PPT}} C_{\mathcal{M} \circ \tilde{\mathcal{T}}_A}] = (1 - p) \lambda_- + \frac{p}{d^4}. \quad (3.56)$$

In this case the addition of the depolarized term that makes the map  $\mathcal{T}_A$  physically implementable introduces only a constant shift in the expectation value of  $W_{\text{PPT}}$ . As a result, for any PPT unital map  $\mathcal{M}_{\text{unital}}^{\text{PPT}}$  we have

$$\text{Tr}[W_{\text{PPT}} C_{\mathcal{M}_{\text{unital}}^{\text{PPT}} \circ \tilde{\mathcal{T}}_A}] \geq \frac{p}{d^4}. \quad (3.57)$$

Therefore, if we know a priori that the map  $\mathcal{M}$  to be detected is a unital map, then we are guaranteed that it is a NPT map whenever the expectation value of  $W_{\text{PPT}}$  is smaller than  $p/d^4$ .

As an illustrative example we consider again the case of the CNOT gate. Here we want to detect such a gate as a NPT map by following the experimental procedure discussed above. It is straightforward to see that the Choi state  $C_{\text{CNOT}_{\mathcal{T}}}$  corresponding to the map  $\text{CNOT}_{\mathcal{T}} = \mathcal{T}_A \circ \text{CNOT} \circ \mathcal{T}_A$  has a single negative eigenvalue  $\lambda_- = -1/2$ . Since the CNOT is unital, from Eq. (3.56) it follows that  $\text{Tr}[W_{\text{PPT}} C_{\text{CNOT} \circ \tilde{\mathcal{T}}_A}] = 0$ , and the gap with the bound provided by Eq. (3.57) ( $\simeq 0.055$  in this case) is then experimentally accessible.

### 3.6 Completely co-positive channels

In this section we consider the set of completely co-positive (CCOP) channels [74]. CCOP channels are of great interest as they are connected via the Choi-Jamiołkowski isomorphism to PPT states [72].



### 3. Quantum Channel Detection

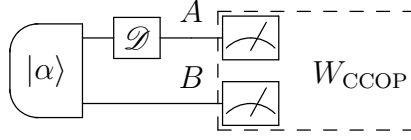


Figure 3.8: Experimental scheme showing the detection of the dephasing channel  $\mathcal{D}$  as a non CCOP channel. Notice that the expectation value of  $W_{\text{CCOP}}$ , namely  $\text{Tr}[W_{\text{CCOP}}C_{\mathcal{D}}]$ , can be measured locally.

A CP map  $\mathcal{C}$  acting on a qudit is CCOP if and only if the composite map  $\mathcal{C}_{\mathcal{T}} = \mathcal{T} \circ \mathcal{C}$ , where  $\mathcal{T}$  is the transposition map, is CP. Since a quantum map is CP if and only if the corresponding Choi operator is positive, we can restate the above definition as follows: a CP map  $\mathcal{C}$  is CCOP if and only if the Choi operator  $C_{\mathcal{C}_{\mathcal{T}}}$  related to the composite map  $\mathcal{C}_{\mathcal{T}}$  is positive.

By the above correspondence we develop a method to detect whether a map is non CCOP by adapting techniques developed for the detection of NPT entangled states [72]. Consider then a map  $\mathcal{M}$  that does not belong to the set of CCOP channels. From the above definition it follows that the bipartite Choi state  $C_{\mathcal{M}_{\mathcal{T}}} = (\mathcal{T}_A \otimes \mathcal{I})[C_{\mathcal{M}}]$  has at least one negative eigenvalue. Let  $\lambda_-$  be the most negative eigenvalue corresponding to the eigenvector  $|\lambda_- \rangle$ . The following operator, i.e.

$$W_{\text{CCOP}} = |\lambda_- \rangle \langle \lambda_-|^{\mathcal{T}_A}, \quad (3.58)$$

is thus suitable to detect the NPT state  $C_{\mathcal{M}_{\mathcal{T}}}$  corresponding to the non CCOP map  $\mathcal{M}_{\mathcal{T}}$ . Notice that the transposition map on the Choi state acts only on the first qudit, i.e.  $\mathcal{T}_A$ .

As an illustrative example we consider the case of the dephasing noise  $\mathcal{D}$  acting on a single qubit, defined by the following CP-TP map

$$\mathcal{D}[\rho] = p\rho + (1-p)Z\rho Z, \quad (3.59)$$

where  $Z$  is a Pauli operator. It is easy to see that the Choi state  $C_{\mathcal{D}}$  corresponding to  $\mathcal{D}$  takes the form

$$C_{\mathcal{D}} = p|\alpha \rangle \langle \alpha| + (1-p)|\phi^- \rangle \langle \phi^-|, \quad (3.60)$$

with  $|\phi^- \rangle = \frac{1}{\sqrt{2}}(|00 \rangle - |11 \rangle)$ . The above state can be shown to be NPT whenever  $p \neq 1/2$ . It is then possible to derive the following detection operator [57, 58] from Eq. 3.58:

$$W_{\text{CCOP}} = \begin{cases} \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + X \otimes X + Y \otimes Y - Z \otimes Z) & \text{for } p < \frac{1}{2}, \\ \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} - X \otimes X - Y \otimes Y - Z \otimes Z) & \text{for } p > \frac{1}{2}. \end{cases} \quad (3.61)$$

This method can be experimentally implemented by preparing a two-qubit state in the maximally entangled state  $|\alpha \rangle$ , then operating with the quantum channel  $\mathcal{D}$  to be detected on one of the two qubits and measuring the operator  $W_{\text{CCOP}}$  acting on both qubits at the end (see Fig. 3.8). If the resulting average

value  $\text{Tr}[W_{\text{CCOP}}C_{\mathcal{D}}]$  is negative, we can then conclude that the Choi state  $C_{\mathcal{D}\mathcal{T}} = \mathcal{T} \circ \mathcal{D}$  is NPT and that the channel  $\mathcal{D}$  under consideration is not CCOP.

Finally, we would like to stress that, since every NPT state is entangled, the detection of a non CCOP channel  $\mathcal{M}$  implies that  $\mathcal{M}$  is not EB as well, however the opposite does not hold in general. Actually the set of EB channels is a subset of the CCOP channels, and the two sets coincide only when the channels act on two-dimensional systems. From the perspective of QCD, this implies that for higher dimensional systems a quantum channel detected as non EB may nevertheless belong to the set of CCOP maps.

### 3.7 Bi-entangling operations

In this section we focus on bi-entangling (BE) operations, a class of quantum maps that can generate at most bipartite entanglement. They were introduced in Ref. [75] in the context of quantum computation and were shown to be efficiently simulatable classically. BE operations are quantum maps acting on two qudit systems  $AB$  in such a way that they can be expressed as convex combinations of (a) separable operations, (b) operations that swap the two qudits and then act as a separable operation, and (c) EB channels, that break any entanglement between the two qudits on which the channel acts and extra ancillae [75]. Via the Choi-Jamiołkowski isomorphism we can then characterize the set of BE operations in terms of the corresponding Choi states.

Consider a BE operation  $\mathcal{M}_{BE}$  acting on the bipartite system  $AB$ , not necessarily TP. The Choi state  $C_{\mathcal{M}_{BE}}$  associated to  $\mathcal{M}_{BE}$  is then a four-partite state (composed of subsystems  $A, B, C$  and  $D$ ). Separable maps have separable Choi states with respect to the bipartition  $AC|BD$  [25]. As a consequence, maps of type (b), with a swap gate followed by separable maps, have separable Choi states in  $AD|BC$ . EB channels correspond to separable Choi states in the bipartition  $AB|CD$ . A general Choi state  $C_{\mathcal{M}_{BE}}$  for a BE map can then be written as a convex combination of four-partite states biseparable with respect to bipartitions  $AC|BD$ ,  $AD|BC$  and  $AB|CD$ , namely

$$C_{\mathcal{M}_{BE}} = p \sum_i p_i C_i^{(AC|BD)} + q \sum_j q_j C_j^{(AD|BC)} + r \sum_k r_k C_k^{(AB|CD)}, \quad (3.62)$$

where  $(p, q, r)$ ,  $\{p_i\}$ ,  $\{q_j\}$  and  $\{r_k\}$  are probability distributions. Notice that the first term corresponds to the set (a), the second to (b) and the third to (c). In other words, the Choi states  $C_{\mathcal{M}_{BE}}$  corresponding to BE operations lie in the convex hull of states biseparable with respect to the bipartitions  $AC|BD$ ,  $AD|BC$  and  $AB|CD$  for the four-partite system  $ABCD$ . We name this convex set of four-partite Choi states corresponding to BE operations as  $S_{BE}$ . It is now possible to develop detection procedures for BE operations by employing suitable operators that detect the corresponding Choi state with respect to the biseparable states belonging to  $S_{BE}$ .

### 3. Quantum Channel Detection

---

We now focus on the case of a non BE unitary  $U$  acting on two qudits. The corresponding Choi state is pure and given by  $|U\rangle = (U \otimes \mathbb{1}) |\alpha\rangle$ . Therefore, a suitable detection operator for  $U$  as a non BE operation can be constructed as

$$W_{BE} = \alpha_{BE}^2 \mathbb{1} - C_U, \quad (3.63)$$

where  $C_U = |U\rangle \langle U|$ , and the coefficient  $\alpha_{BE}$  is the overlap between the closest biseparable state in the set  $S_{BE}$  and the entangled state  $|U\rangle$ , namely

$$\alpha_{BE}^2 = \max_{\mathcal{M}_{BE}} \langle U | C_{\mathcal{M}_{BE}} | U \rangle. \quad (3.64)$$

Since the maximum of a linear function over a convex set is always achieved on the extremal points, the maximum involved in  $\alpha_{BE}$  can be always calculated by maximizing over the pure biseparable states in  $S_{BE}$ , i.e.

$$\alpha_{BE} = \max_{|\Xi\rangle \in S_{BE}} |\langle \Xi | U \rangle|. \quad (3.65)$$

By exploiting the Schmidt decomposition [1] of the state  $|U\rangle$ , the maximization above can be expressed analytically as

$$\alpha_{BE} = \max_i \max_{\lambda} \lambda_i(U), \quad (3.66)$$

where the index  $i$  labels the bipartitions  $AC|BD$ ,  $AD|BC$  and  $AB|CD$ , and  $\lambda_i(U)$  are the Schmidt coefficients of  $|U\rangle$  in the bipartition  $i$ . Therefore, in order to find the coefficient  $\alpha_{BE}$  one has to find the maximal Schmidt coefficient of  $|U\rangle$  for a fixed bipartite splitting, and then maximize it among all the bipartitions involving only two versus two subsystems.

As an example of the above procedure consider the following unitary operation  $V$  acting on a two-qubit system

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (3.67)$$

Notice that the gate  $V$  is a modified swap gate such that it is no longer a BE operation. The coefficient  $\alpha_{BE}$  for  $V$  can be computed following the steps outlined above. The Choi state  $|V\rangle$  associated to the gate  $V$  is given by

$$|V\rangle = \frac{1}{\sqrt{2}} (|\alpha\rangle_{AD} |00\rangle_{BC} + |\phi^-\rangle_{AD} |11\rangle_{BC}), \quad (3.68)$$

and the Schmidt coefficients of  $V$  with respect to the bipartitions  $AC|BD$ ,  $AD|BC$  and  $AB|CD$  can be easily computed as  $\lambda_{AC|BD}(V) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ ,  $\lambda_{AD|BC}(V) = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0)$  and  $\lambda_{AB|CD}(V) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ . Therefore, the coefficient  $\alpha_{BE}$  equals  $1/\sqrt{2}$  and a suitable detection operator in order to detect  $V$  as a non BE operation takes the form

$$W_{BE} = \frac{1}{2} \mathbb{1} - C_V. \quad (3.69)$$

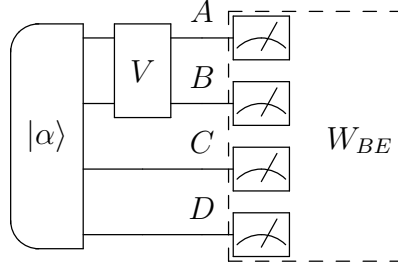


Figure 3.9: Experimental scheme implementing the detection of the gate  $V$  defined in Eq. 3.67 as a non BE operation.

From an experimental point of view, the detection procedure can be implemented as follows: prepare a four-qubit system in the state  $|\alpha\rangle = |\alpha\rangle_{AC} |\alpha\rangle_{BD}$ , apply the quantum gate  $V$  to qubits  $A$  and  $B$ , and finally perform a suitable set of local measurements in order to measure the operator (3.69). If the resulting average value  $\text{Tr}[W_{BE}C_V]$  is negative then the quantum map is detected as a non BE operation. The experimental scheme is shown in Fig. 3.9.

We conclude this section by noticing that the method described above leads to different detection operators with respect to the detection method for non separable maps developed in Sec. 3.4. Indeed, the optimal detection operator that reveals the gate  $V$  as a non separable map is

$$W_S = \frac{1}{4} \mathbb{1} - C_V. \quad (3.70)$$

Already in the two-qubit case the operator above is stronger than  $W_{BE}$  in Eq. (3.69), in the sense that it has a negative expectation value for a larger set of quantum maps. This is actually due to the fact that BE maps are a strict subset of separable maps (since the set of separable Choi states in the bipartition  $AC|BD$  is a strict subset of  $S_{BE}$ ).

## 3.8 Summary and further developments

In summary we have presented an experimentally feasible method to detect several sets of quantum channels. The proposed procedure works when some a priori knowledge on the quantum channel is available and is based on a link to detection methods for entanglement properties of multipartite quantum states via witness operators.

The method has been first explicitly illustrated in the simple case of EB channels, and then presented to detect separability properties of quantum channels. In particular, methods to reveal non SRUs and non separable maps have been derived, showing also the possibility to detect the gap between the sets of SRUs and separable maps. This result highlights a richer separability structure of Choi operators that has no counterpart in the separability properties of ordinary entangled/separable states. The present method has been

### 3. Quantum Channel Detection

---

applied also to detect other properties of quantum maps that rely on a convex structure and reflect on properties of the corresponding Choi states, such as, for example, PPT and CCOP channels, and BE operations.

The advantage over standard quantum process tomography is that a much smaller number of measurement settings is needed in an experimental implementation. Finally, we want to point out that the proposed scheme can be implemented with current technology, for instance in a quantum optical scheme [76, 77].

# Chapter 4

## Map Detection: Noise Robustness and Experimental Realization

The experimental realization of a quantum channel is unavoidably affected by noise. One possible way to check how well this has been achieved is to make a full tomography of the process. This nevertheless is known to be very expensive in terms of number of measurements to be performed [1]. Since in many practical situations, one is only interested in some specific properties of the channel, a more suitable approach is the quantum channel detection (QCD) method developed in the previous chapter. The method allows to detect properties of quantum channels when some a priori knowledge about the form of the channel is available.

In this chapter we illustrate in detail the QCD method for detecting non separable maps and consider in particular the explicit examples of the CNOT and CZ gates. We analyse their robustness in the presence of noise for several quantum noise models, namely depolarising, dephasing, bit flip and amplitude damping noise [28]. We then demonstrate experimentally the possibility of efficiently detecting properties of quantum channels and quantum gates via the above QCD method. The optimal detection scheme is first achieved for non entanglement breaking (EB) channels of the depolarizing form and is based on the generation and detection of polarized entangled photons. We then demonstrate channel detection for non separable maps by considering the CNOT gate and employing two-photon hyperentangled states [29].

### 4.1 Detecting the CNOT and CZ gates

In this section we briefly remind how the channel detection method works in the case of separable random unitary (SRU) and separable maps.

Consider the case of detecting a non separable unitary operation  $U$  acting

#### 4. Map Detection: Noise Robustness and Experimental Realization

---

on a bipartite system  $AB$ . As explained in Secs. 3.3 and 3.4, a suitable detection operator can be constructed as

$$W_U = \beta \mathbb{1} - C_U, \quad (4.1)$$

where  $\beta$  is an appropriately chosen coefficient, and  $C_U = |U\rangle\langle U|$  is the projector on the Choi state corresponding to the unitary  $U$ , i.e.  $|U\rangle = (U \otimes \mathbb{1})|\alpha\rangle$ . The choice of  $\beta$  depends on the set we want to rule out: if we want to detect the unitary  $U$  as a non SRU map, we set  $\beta = \alpha_{SRU}^2$  given by Eq. (3.22), while if we aim at revealing  $U$  as a non separable map, we choose  $\beta = \alpha_S^2$  defined in Eq. (3.32). Notice that generally  $\alpha_S \geq \alpha_{SRU}$ , except in the two-qubit case where the inequality always holds. Thus, as far as quantum channels acting on two qubits are concerned, there is no chance to detect the gap between the sets of separable and SRU maps. Throughout this chapter we mainly focus on the case of two qubits, we then prefer to talk about the detection of  $U$  as a non separable channel instead of as a non SRU, since the condition of non separability is stronger than the condition of not being SRU.

We now specify the above construction to the particular case of the CNOT gate acting on two qubits. As discussed in the previous chapter, the general detection operator (4.1) takes the form

$$W_{\text{CNOT}} = \frac{1}{2} \mathbb{1} - C_{\text{CNOT}}, \quad (4.2)$$

with  $C_{\text{CNOT}} = |\text{CNOT}\rangle\langle\text{CNOT}|$ . Notice that the detection operator  $W_{\text{CNOT}}$  above can be decomposed into a linear combination of local operators as already shown in Eq. (3.28).

As a second significant example consider the CZ operation, which also represents an important two-qubit gate in quantum computation [1]. This operation is defined as

$$\text{CZ} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & Z \end{pmatrix}, \quad (4.3)$$

namely it has the same structure as the CNOT gate, with  $X$  replaced by  $Z$ . This case can be connected to the detection procedure for the CNOT gate by exploiting the following relation between the CNOT and CZ gates

$$\text{CZ} = (\mathbb{1} \otimes H) \text{CNOT} (\mathbb{1} \otimes H), \quad (4.4)$$

where  $H$  is the Hadamard gate, defined as  $H = \frac{1}{\sqrt{2}}(X + Z)$ . Since the two gate operations differ only by a local unitary transformation, the maximization performed in the calculation of  $\alpha_{SRU} = \alpha_S$  leads to the same value  $\beta = 1/2$ . The corresponding detection operator  $W_{\text{CZ}}$  can then be written as

$$W_{\text{CZ}} = \frac{1}{2} \mathbb{1} - C_{\text{CZ}}, \quad (4.5)$$

which can be easily decomposed into local Pauli operators as follows:

$$\begin{aligned}
 W_{CZ} = \frac{1}{64} & (3\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} - \mathbb{1}Z\mathbb{1}Z - Z\mathbb{1}Z\mathbb{1} - ZZZZ \\
 & - ZX\mathbb{1}X + ZY\mathbb{1}Y - \mathbb{1}XZX + \mathbb{1}YZY \\
 & - XZX\mathbb{1} - X\mathbb{1}XZ + YZY\mathbb{1} + Y\mathbb{1}YZ \\
 & - YYXX - YXXY - XYYX - XYYX). \quad (4.6)
 \end{aligned}$$

Notice that, besides the convenient implementation in terms of local operators, an other important aspect to study is how much noise the detection operator  $W_U$  of (4.1) tolerates. In the next section we will show several cases in which the presence of noise is taken into account. The map we want to detect is thus no longer considered as a perfect CNOT (or CZ) gate but instead as a sort of composite map representing the CNOT (or CZ) with in addition several kinds of quantum noise.

## 4.2 Noise robustness

We now study the robustness of the method in the presence of additional noise, which can influence the operation of the quantum channel. The situation we have in mind is the following. Suppose we are given an operator  $W_U$  of the form (4.1) to detect a unitary  $U$  acting on two qubits. Suppose also that the experimental implementation of  $U$  leads to a new noisy map  $\mathcal{M}$ , which is close to the original  $U$  by construction but not exactly  $U$  due to the presence of noise. Does  $W_U$  still detect the map  $\mathcal{M}$  as non separable?

Since the expectation value of the operator  $W_U$  is continuous with respect to the Choi state  $C_{\mathcal{M}}$ , we expect an affirmative answer for maps enough close to the target unitary  $U$ . However, to quantify how close to  $U$  a noisy map  $\mathcal{M}$  should be in order to be detected by our method, we have to check whether the expectation value of  $W_U$  on  $\mathcal{M}$ , i.e.

$$\text{Tr}[W_U C_{\mathcal{M}}] = \beta - \text{Tr}[C_{\mathcal{M}} C_U], \quad (4.7)$$

is negative. To this end, let us notice that the overlap between two Choi states  $C_{\mathcal{L}}$  and  $C_{\mathcal{M}}$  corresponding to the maps  $\mathcal{L}$  and  $\mathcal{M}$  acting on  $\mathcal{D}(\mathcal{H})$  can be generally written as

$$\text{Tr}[C_{\mathcal{M}} C_{\mathcal{L}}] = \frac{1}{d^2} \sum_{i,j=1}^d \text{Tr}[\mathcal{M}(|i\rangle\langle j|) \mathcal{L}(|j\rangle\langle i|)], \quad (4.8)$$

where  $\{|i\rangle\}$  represents the computational basis for the Hilbert space  $\mathcal{H}$  with arbitrary finite dimension  $d$ . In terms of the Kraus operators  $\{A_k\}$  and  $\{B_l\}$  of the maps  $\mathcal{M}$  and  $\mathcal{L}$ , respectively, the above expression can be rewritten as

$$\text{Tr}[C_{\mathcal{M}} C_{\mathcal{L}}] = \frac{1}{d^2} \sum_{k,l} |\text{Tr}[A_k^\dagger B_l]|^2, \quad (4.9)$$



#### 4. Map Detection: Noise Robustness and Experimental Realization

where the double summation is over the Kraus operators and the absolute value comes from the identity  $\text{Tr}[A^\dagger] = \text{Tr}[A]^*$ .

In the case which we are interested in,  $\mathcal{H}$  is a two-qubit system of dimension  $d = 4$  and  $\mathcal{L}$  is given by a unitary operation  $U$ . Therefore, the above expression takes the form

$$\text{Tr}[C_{\mathcal{M}}C_U] = \frac{1}{16} \sum_k |\text{Tr}[A_k^\dagger U]|^2, \quad (4.10)$$

where the summation is now performed just over the Kraus operators  $\{A_k\}$  of the noisy map  $\mathcal{M}$ . The expectation value for the detection operator  $W_U$  detecting the gate  $U$  can then be rewritten as

$$\text{Tr}[W_U C_{\mathcal{M}}] = \beta - \frac{1}{16} \sum_k |\text{Tr}[A_k U^\dagger]|^2. \quad (4.11)$$

In this context, the general map  $\mathcal{M}$  thus represents a noisy implementation of the unitary  $U$  by considering no longer a noiseless gate but adding some quantum noise such as the depolarising, the dephasing, the bit flip or the amplitude damping noise. In the following subsections we will treat these four different noisy processes, and derive some bounds on the amount of noise that the operators  $W_{\text{CNOT}}$  and  $W_{\text{CZ}}$ , constructed to detect gates CNOT and CZ, respectively, can tolerate.

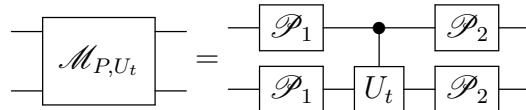
##### 4.2.1 Depolarising noise

We consider first the case of depolarising noise  $\mathcal{P}$ , whose action is described by a CP-TP map of the following form

$$\Gamma_q[\rho] = \sum_{i=0}^3 p_i \sigma_i \rho \sigma_i \quad (4.12)$$

where  $\sigma_0 = \mathbb{1}$  is the identity operator, and  $\{\sigma_i\}$  ( $i = 1, 2, 3$ ) are the three Pauli operators  $\sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z$  respectively. In the case of depolarising noise we have  $p_0 = 1 - 3q/4$  (with  $q \in [0, 1]$ ), while  $p_i = q/4$  for  $i = 1, 2, 3$ , and therefore the parameter  $q$  uniquely describes the depolarising channel.

The presence of noise in the general scenario of a controlled  $C-U_t$  unitary operation can be depicted as follows:



$$\text{---} \boxed{\mathcal{M}_{P,U_t}} \text{---} = \text{---} \begin{array}{c} \boxed{\mathcal{P}_1} \text{---} \bullet \text{---} \boxed{\mathcal{P}_2} \\ \boxed{\mathcal{P}_1} \text{---} \boxed{U_t} \text{---} \boxed{\mathcal{P}_2} \end{array} \text{---}. \quad (4.13)$$

Here,  $U_t$  is the unitary operation acting on the target qubit (in the cases of the CNOT and CZ gates it is given by  $X$  and  $Z$ , respectively), and each depolarizing channel  $\mathcal{P}_i$  involves the parameter  $q_i$ . Notice that  $q_1$  and  $q_2$  are related to the depolarising channels  $\mathcal{P}_1$  and  $\mathcal{P}_2$ . Furthermore, the four depolarizing processes act independently and are assumed to have the same strength ( $q_1$

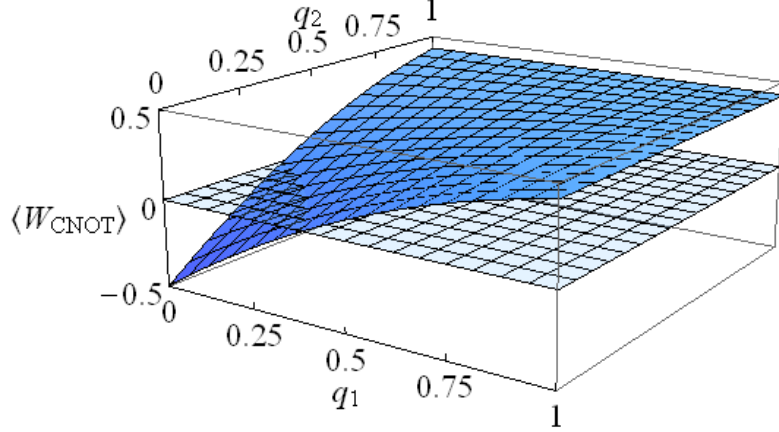


Figure 4.1: Expectation value of  $W_{\text{CNOT}}$  on the noisy state  $C_{\mathcal{M}_{P,X}}$ , i.e.  $\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{P,X}}]$ , in terms of the two noise parameters  $q_1$  and  $q_2$ . Notice that the same plot is obtained for the expectation value of  $W_{\text{CZ}}$  on the Choi state  $C_{\mathcal{M}_{P,Z}}$  corresponding to the noisy map  $\mathcal{M}_{P,Z}$ .

( $q_2$ ) before (after) the controlled operation  $\text{C-}U_t$  for the two qubits. Besides not being so restrictive from a physical perspective, this assumption simplifies a bit the following calculations. The Kraus operators of the tensor product map  $\mathcal{P}_i \otimes \mathcal{P}_i$ , denoted by  $\{P_k^i\}$ , are obviously given by the tensor product of the corresponding Kraus operators of the single-qubit depolarising channel. Notice that the global resulting noisy channel  $\mathcal{M}_{P,U_t}$  shown above is still a random unitary channel.

We first start from the detection of noisy CNOT gate via the operator  $W_{\text{CNOT}}$  given by Eq. (4.2). From Eq. (4.10), we can compute the overlap between the noiseless Choi state  $C_{\text{CNOT}}$  and the Choi operator  $C_{\mathcal{M}_{P,X}}$ , corresponding to the noisy composite map  $\mathcal{M}_{P,X}$  given by (4.13) with  $U_t = X$ , as

$$\text{Tr}[C_{\mathcal{M}_{P,X}}C_{\text{CNOT}}] = \frac{1}{16} \sum_{k,l} |\text{Tr}[P_k^1 \text{CNOT} P_l^2 \text{CNOT}]|^2, \quad (4.14)$$

where  $\{P_k^1\}$  and  $\{P_l^2\}$  are the Kraus sets of  $\mathcal{P}_1 \otimes \mathcal{P}_1$  and  $\mathcal{P}_2 \otimes \mathcal{P}_2$ , respectively. By performing the calculation explicitly and remembering that, apart from the parameters  $q_i$ , the term on the right hand side above is a symmetric matrix in  $k, l$ , we arrive at the following expression for the expectation value

$$\begin{aligned} \text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{P,X}}] = \\ \frac{1}{2} - \frac{1}{16}(16\bar{q}_1^2\bar{q}_2^2 + 2q_1\bar{q}_1q_2\bar{q}_2 + q_1^2q_2\bar{q}_2 + q_1\bar{q}_1q_2^2 + \frac{5}{16}q_1^2q_2^2), \end{aligned} \quad (4.15)$$

with the definition  $\bar{q}_i = 1 - \frac{3q_i}{4}$  for  $i = 1, 2$  (see Fig. 4.1).

Let us now study some special cases of the above situation. Suppose first that  $q_2 = 0$ , so that the noise affects the channel only before the CNOT. In

this case the expectation value becomes

$$\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{P,X}}] = \frac{1}{2} - \bar{q}_1^2, \quad (4.16)$$

which is negative for  $q_1 < \frac{4-2\sqrt{2}}{3} \simeq 0.39$ . Therefore, the values of  $q_1$  below this threshold lead to a detection of the CNOT gate as a non separable channel. Since the situation is symmetric, the same obviously holds when  $q_1 = 0$  and we are looking at  $q_2$ , namely the action of the depolarising channel either before or after the CNOT operation leads to the same result. Another interesting situation is when both the channels before and after the CNOT gate introduce the same level of noise, namely when  $q_1 = q_2 = q$ . In this case we get the following expression for the expectation value

$$\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{P,X}}] = \frac{1}{2} - \frac{1}{16}(q-2)^2(5q^2 - 8q + 4). \quad (4.17)$$

The CNOT gate is thus detected as a non separable map when  $q < 0.21$ . Notice that the threshold in this case is not as high as the one we obtained before, since the situation is much noisier because two sources of noise are now present.

We now consider the case of the CZ gate. The detection of noisy CZ gate via  $W_{\text{CZ}}$  turns out to give the same threshold of noise as for the CNOT gate. This is basically due to the symmetry properties of the depolarising noise, which acts isotropically along the three directions of the Pauli matrices. It is then straightforward to find that the expectation value of  $W_{\text{CZ}}$  on  $C_{\mathcal{M}_{P,Z}}$ , namely  $\text{Tr}[W_{\text{CZ}}C_{\mathcal{M}_{P,Z}}]$  is exactly given by Eq. (4.15). Hence, the analysis we have performed in that case still holds for the CZ gate.

As we can see, the presence of local depolarising noise thus affects the CNOT and CZ operations in such a way that, beyond a certain amount of noise, the noisy CNOT and CZ operations are no longer detected as non separable by our method.

### 4.2.2 Dephasing noise

Let us now assume that dephasing noise is present, acting independently on the two qubits  $A$  and  $B$  in general both before and after the unitary we want to detect, namely

$$\begin{array}{c} \text{---} \boxed{\mathcal{M}_{D,U_t}} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \boxed{\mathcal{D}_1} \text{---} \bullet \text{---} \boxed{\mathcal{D}_2} \text{---} \\ \text{---} \boxed{\mathcal{D}_1} \text{---} \boxed{U_t} \text{---} \boxed{\mathcal{D}_2} \text{---} \end{array}, \quad (4.18)$$

where  $U_t$  is again either  $X$  or  $Z$ . Phase damping noise is described by a CP-TP map of the form (4.12) where the probabilities are now given by  $p_0 = 1 - q$ ,  $p_1 = p_2 = 0$  and  $p_3 = q$ . Notice that in this case the global resulting channel  $\mathcal{M}_{D,U_t}$  is still a random unitary channel.

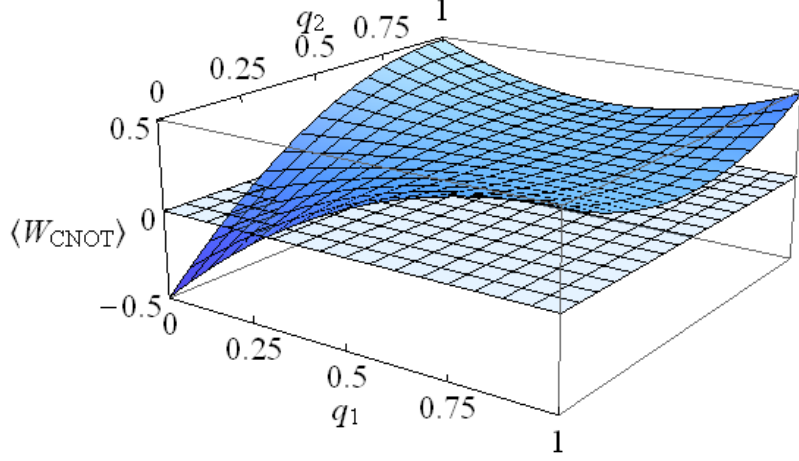


Figure 4.2: Expectation value  $\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{D,X}}]$  of  $W_{\text{CNOT}}$  on the noisy state  $C_{\mathcal{M}_{D,X}}$  as a function of the two noise parameters  $q_1$  and  $q_2$ . Notice that the same behaviour of  $W_{\text{CNOT}}$  is obtained for the noisy map  $\mathcal{M}_{B,X}$ , i.e. when bit flip noise is concerned.

In order to quantify the noise robustness of the detection operator  $W_{\text{CNOT}}$  with respect to dephasing noise, we calculate the expectation value of  $W_{\text{CNOT}}$  given by Eq. (4.2) with respect to the state  $C_{\mathcal{M}_{D,X}}$ , i.e. the Choi state corresponding to the composite map  $\mathcal{M}_{D,X} = (\mathcal{D}_2 \otimes \mathcal{D}_2)\text{CNOT}(\mathcal{D}_1 \otimes \mathcal{D}_1)$  depicted in (4.18) with  $U_t = X$ . The problem thus reduces to evaluate the overlap between the Choi states  $C_{\text{CNOT}}$  and  $C_{\mathcal{M}_{D,X}}$ . By using Eq. (4.11), this procedure leads to the formula

$$\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{D,X}}] = \frac{1}{2} - [(1 - q_1)^2(1 - q_2)^2 + q_1q_2(1 - q_1q_2)], \quad (4.19)$$

that is plotted in Fig. 4.2 for an immediate reading.

From Fig. 4.2 we can see that  $\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{D,X}}] < 0$  for certain intervals of the noise parameters  $q_1$  and  $q_2$ . From the symmetry of the expression (4.19), the action of dephasing noise either before or after the CNOT gate leads to the same result. In this case, considering e.g.  $q_2 = 0$ , the expectation value of  $W_{\text{CNOT}}$  is negative for  $q_1 < 1 - \frac{1}{\sqrt{2}} \simeq 0.29$ . When instead the dephasing channels introduce the same level of noise ( $q_1 = q_2 = q$ ) the expectation value of  $W_{\text{CNOT}}$  turns out to be negative for  $q < 0.17$  and, therefore the CNOT operation can be detected in this range.

Regarding the robustness of the detection operator  $W_{\text{CZ}}$ , we need to compute the expectation value of  $W_{\text{CZ}}$  with respect to the Choi state  $C_{\mathcal{M}_{D,Z}}$ , representing the noisy implementation of the CZ gate, i.e.  $\mathcal{M}_{D,Z} = (\mathcal{D}_2 \otimes \mathcal{D}_2)\text{CZ}(\mathcal{D}_1 \otimes \mathcal{D}_1)$ . Following the same calculation as before we get

$$\text{Tr}[W_{\text{CZ}}C_{\mathcal{M}_{D,Z}}] = \frac{1}{2} - (1 - q_1 - q_2 + 2q_1q_2)^2, \quad (4.20)$$

which differs very much from the expectation value calculated for the CNOT gate, compare Figs. 4.2 and 4.3.

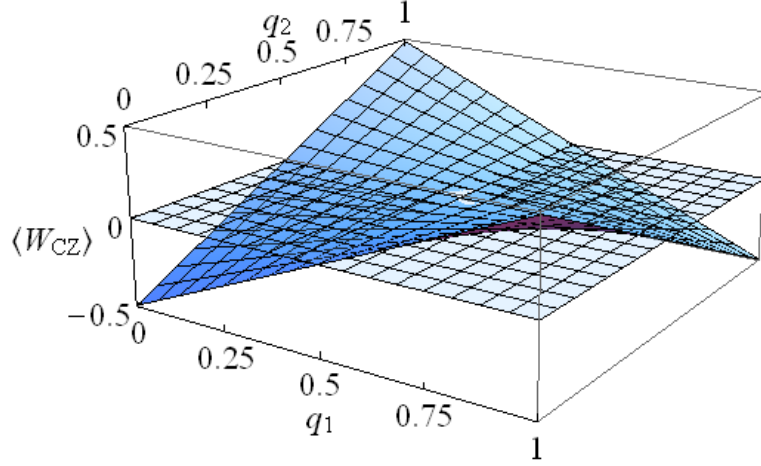


Figure 4.3: Expectation value of the detection operator  $W_{CZ}$  on the noisy state  $C_{\mathcal{M}_{D,Z}}$  in terms of the two noise parameters  $q_1$  and  $q_2$ . Notice that when  $q_1 = q_2 = q$ , the expectation value  $\text{Tr}[W_{CZ}C_{\mathcal{M}_{D,Z}}]$  is negative for high level of noise  $q$  as well.

Also in this case, see Fig. 4.3, if the noise is present just before or after the gate, namely  $q_2 = 0$  or  $q_1 = 0$ , our method detects the noisy CZ as a non separable map if  $q_1 < 1 - \frac{1}{\sqrt{2}} \simeq 0.29$  (or  $q_2 < 1 - \frac{1}{\sqrt{2}} \simeq 0.29$ ). This threshold is exactly the same as the one found for  $W_{\text{CNOT}}$ , thus the operator for detecting the CZ turns out to be as robust against dephasing noise as  $W_{\text{CNOT}}$  revealing CNOT. If the two sources of noise have the same strength, i.e.  $q_1 = q_2 = q$ , then the expectation value turns out to be negative if the noise level is either  $q < \frac{1}{2}(1 - \sqrt{1 - \sqrt{2}}) \simeq 0.18$  or  $q > \frac{1}{2}(1 + \sqrt{1 - \sqrt{2}}) \simeq 0.82$ . This behaviour may seem to be very surprising, since it follows that  $W_{CZ}$  can tolerate not only low levels of noise but high levels too. The only regime where it fails is when the noise has a medium strength. However, this effect can be intuitively explained as follows. Dephasing noise always commutes with the CZ gate, thus the noise can be thought to be applied twice before the regarded gate. For high noise level  $q$ , the action of two consecutive dephasing processes leads almost to the identical map, since  $Z^2 = 1$ , and so the scenario can be thought as noiseless. We want to stress that this result is completely different from the one obtained for  $W_{\text{CNOT}}$  since there only a low amount of noise was tolerated.

### 4.2.3 Bit flip noise

Another interesting model of noise is given by bit flip noise  $\mathcal{B}$ , defined as a CP-TP map of the form (4.12) with probabilities  $p_0 = 1 - q$ ,  $p_1 = q$  and  $p_2 = p_3 = 0$ . As before, we consider the situation in which the noise acts independently on the two qubits both before and after the controlled operation

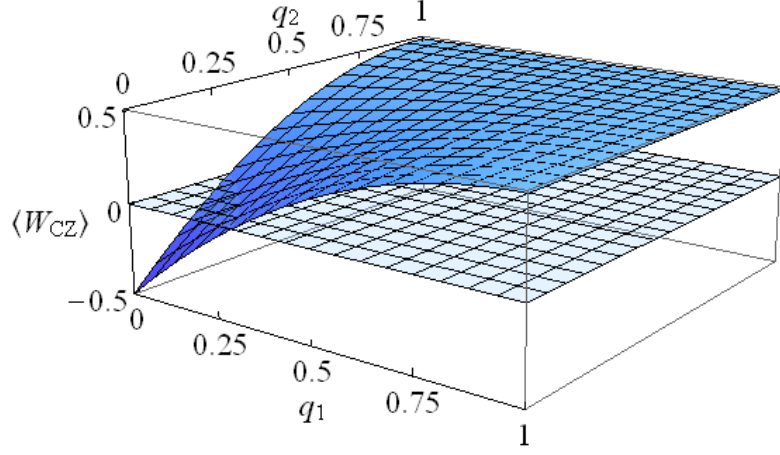


Figure 4.4: Expectation value of the detection operator  $W_{CZ}$  on the noisy state  $C_{\mathcal{M}_{B,Z}}$  as a function of the two noise parameters  $q_1$  and  $q_2$ .

C- $U_t$  (either CNOT or CZ):

$$\begin{array}{c} \boxed{\mathcal{M}_{B,U_t}} \\ \hline \end{array} = \begin{array}{c} \boxed{\mathcal{B}_1} \quad \bullet \quad \boxed{\mathcal{B}_2} \\ | \quad \quad | \\ \boxed{\mathcal{B}_1} \quad \boxed{U_t} \quad \boxed{\mathcal{B}_2} \end{array}. \quad (4.21)$$

Let us first focus on the detection of the CNOT gate by the operator  $W_{\text{CNOT}}$ . By exploiting Eq. (4.11), where the composite map is now given by  $\mathcal{M}_{B,X} = (\mathcal{B}_2 \otimes \mathcal{B}_2)\text{CNOT}(\mathcal{B}_1 \otimes \mathcal{B}_1)$ , we arrive at the following expectation value of  $W_{\text{CNOT}}$  over its noisy implementation  $C_{\mathcal{M}_{B,X}}$ :

$$\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{B,X}}] = \frac{1}{2} - [(1 - q_1)^2(1 - q_2)^2 + q_1q_2(1 - q_1q_2)]. \quad (4.22)$$

This turns out to be the same expectation value as for the case of dephasing noise, therefore the discussion already done below Eq. (4.19) still holds (see also Fig. 4.2).

In order to study the robustness of  $W_{CZ}$  to detect CZ with additional bit flip noise, we have to evaluate the quantity  $\text{Tr}[W_{CZ}C_{\mathcal{M}_{B,Z}}]$  with  $\mathcal{M}_{B,Z} = (\mathcal{B}_2 \otimes \mathcal{B}_2)\text{CZ}(\mathcal{B}_1 \otimes \mathcal{B}_1)$ . By using Eq. (4.11), we get

$$\text{Tr}[W_{CZ}C_{\mathcal{M}_{B,Z}}] = \frac{1}{2} - (1 - q_1)^2(1 - q_2)^2, \quad (4.23)$$

which allows us to derive different thresholds for the noise tolerance of CZ (see Fig. 4.4). If noise is neglected either after ( $q_2 = 0$ ) or before ( $q_1 = 0$ ) the CZ gate, then the method is able to tolerate a level of noise up to  $1 - \frac{1}{\sqrt{2}} \simeq 0.29$ , i.e. either  $q_1 < 1 - \frac{1}{\sqrt{2}}$  or  $q_2 < 1 - \frac{1}{\sqrt{2}}$ . In the case where both the noise sources show the same amount of noise, namely  $q_1 = q_2 = q$ , it follows that the CZ gate is detected as long as  $q < 0.16$ .

### 4.2.4 Amplitude damping noise

As a last noise model we consider the amplitude damping channel, which is not a random unitary noise and it is described by the following Kraus operators acting on a single qubit

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, A_2 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \quad (4.24)$$

where  $\gamma$  is the parameter characterising the amount of damping.

In the case of  $W_{\text{CNOT}}$ , following the same procedure described above and by considering now the composite map  $\mathcal{M}_{A,X} = (\mathcal{A}_2 \otimes \mathcal{A}_2)\text{CNOT}(\mathcal{A}_1 \otimes \mathcal{A}_1)$ , we have

$$\begin{aligned} \text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{A,X}}] = \\ \frac{1}{2} - \frac{1}{16} [(1 + \sqrt{\bar{\gamma}_1\bar{\gamma}_2}(1 + \sqrt{\bar{\gamma}_1} + \sqrt{\bar{\gamma}_2}))^2 + \gamma_1\bar{\gamma}_1\gamma_2\bar{\gamma}_2], \end{aligned} \quad (4.25)$$

where we have defined  $\bar{\gamma} = 1 - \gamma$ . As in the previous cases the above expression is symmetric under exchange of  $\gamma_1$  and  $\gamma_2$ , see Fig. 4.5. When noise acts only either before or after the CNOT gate, e.g.  $\gamma_2 = 0$ , the above expression is negative for  $\gamma_1 < 0.53$ . For the particular case of  $\gamma_1 = \gamma_2 = \gamma$  we get

$$\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{A,X}}] = \frac{1}{2} - \frac{1}{16} [(1 + \bar{\gamma}(1 + 2\sqrt{\bar{\gamma}}))^2 + \gamma^2\bar{\gamma}^2], \quad (4.26)$$

which is negative for  $\gamma < 0.31$ . Therefore the composite map  $\mathcal{M}_{A,X}$  can be detected as non separable in this range of noise parameter  $\gamma$ .

The noise robustness of  $W_{\text{CZ}}$  with respect to the amplitude damping noise can be studied starting from the expectation value of  $W_{\text{CZ}}$  on  $\mathcal{M}_{A,Z} = (\mathcal{A}_2 \otimes$

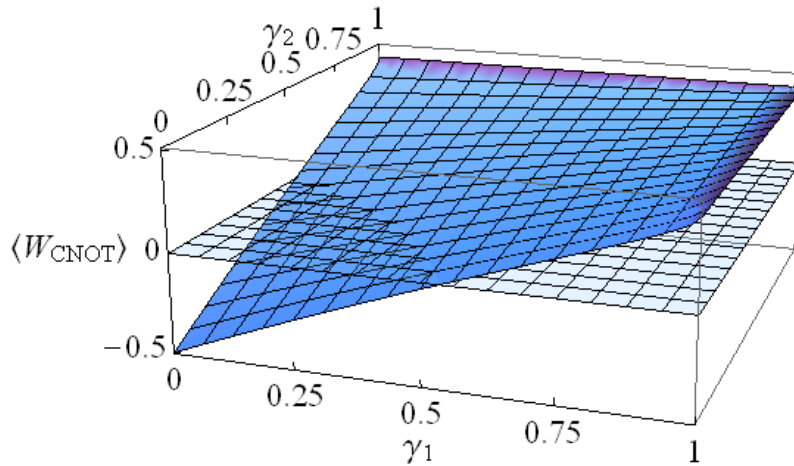


Figure 4.5: Expectation value  $\text{Tr}[W_{\text{CNOT}}C_{\mathcal{M}_{A,X}}]$  of  $W_{\text{CNOT}}$  on the noisy state  $C_{\mathcal{M}_{A,X}}$ , corresponding to the noisy map  $\mathcal{M}_{A,X}$ , in terms of the two damping parameters  $\gamma_1$  and  $\gamma_2$ .

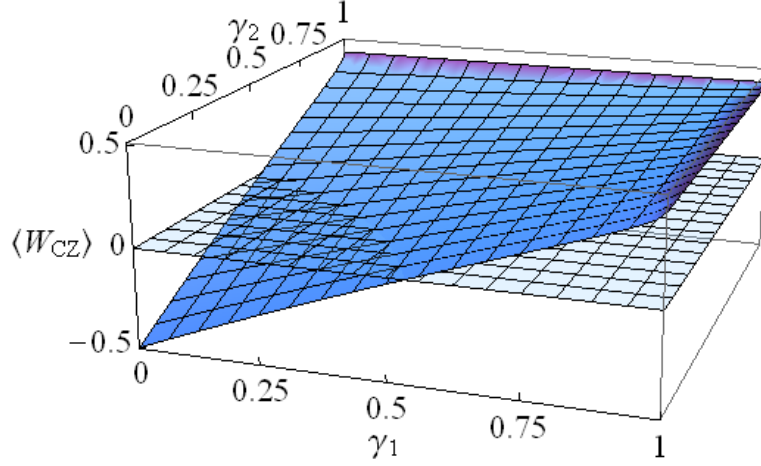


Figure 4.6: Expectation value of  $W_{CZ}$  on the Choi state  $C_{\mathcal{M}_{A,Z}}$  as a function of the two damping parameters  $\gamma_1$  and  $\gamma_2$ . The plotted behaviour is very similar to the behaviour of  $W_{CNOT}$ , but nevertheless it is not exactly the same.

$\mathcal{A}_2)CZ(\mathcal{A}_1 \otimes \mathcal{A}_1)$ , which is given by

$$\text{Tr}[W_{CZ}C_{\mathcal{M}_{A,Z}}] = \frac{1}{2} - \frac{1}{16}(1 + \sqrt{\gamma_1\gamma_2})^4, \quad (4.27)$$

and depicted in Fig. 4.6. As we can see from the above expression, when noise is present only before the CZ gate, i.e.  $\gamma_2 = 0$ , a negative result is found for  $\gamma_1 < 0.53$ , exactly as for  $W_{CNOT}$ . Notice that, since the above expectation value is still invariant under exchange of  $\gamma_1$  and  $\gamma_2$ , the same holds if noise acts just after the controlled gate. When noise before and after the CZ gate is the same, i.e.  $\gamma_1 = \gamma_2 = \gamma$ , it is easy to show that

$$\text{Tr}[W_{CZ}C_{\mathcal{M}_{A,Z}}] = \frac{1}{2} - \frac{1}{16}(1 + \bar{\gamma})^4. \quad (4.28)$$

Thus the operator  $W_{CZ}$  detects the noisy CZ as a non separable map only if  $\gamma < 0.31$ . We would like to stress that this value is the same as before only because we truncate the root of Eq. (4.28) at the second digit.

This last noise model concludes the theoretical study of the robustness of the QCD method against quantum noise. In particular several important noise models have been considered so far, and different thresholds in order for our detection operator to work have been calculated. Notice that one might also face a different noisy situation, namely, when the maximally entangled state  $|\alpha\rangle$ , from which the Choi state  $C_U$  is implemented, is not perfectly prepared. In this case one should consider two different scenarios. On the one hand, if the noise is such that it ruins the purity and the entanglement content of the state  $|\alpha\rangle$ , then it can be suitably recast to the noise models that we have just discussed. In fact, one can always think of the noisy initial state as generated by extra noise processes that act on the perfect input state  $|\alpha\rangle$



before the to-be-detected unitary  $U$  is performed. On the other hand, if the noise is such that it creates not desired entanglement in the splitting  $AC|BD$ , i.e. the initial maximally entangled state  $|\alpha\rangle_{AC}|\alpha\rangle_{BD}$  is no longer biseparable in the bipartition  $AC|BD$ , then the method no longer guarantees to detect non separability. As a result, in an experimental realization of the proposed method, one has to be sure to deal with a proper biseparable initial state  $|\alpha\rangle$  by means of either other detection techniques or quantum state tomography (see Sec. 4.3).

In the next section we will focus on the experimental detection of quantum channels. Channels of the depolarising form and the CNOT gate will be detected as non EB and non separable, respectively. For this latter case, dephasing noise will be added to the system in a controlled way. Therefore, the noise analysis just performed turns out to be useful, and testable in an experimental set-up.

### 4.3 Experimental detection of quantum channels

In this section we focus on the experimental realization of the QCD method previously explained. The QCD scheme is firstly exploited for non EB channels of the depolarizing form and is based on the generation and detection of polarized entangled photons. We then perform the QCD in order to reveal the CNOT gate as a non separable map by employing two-photon hyperentangled states.

#### 4.3.1 Single-qubit EB channels

We now show how to experimentally detect the depolarizing channel  $\Gamma_p$  defined in Eq. (3.7) as a non EB channel. More precisely, as extensively explained in Sec. 3.2, the problem reduces to the detection of the corresponding Choi state

$$C_{\Gamma_p} = (1 - \frac{4}{3}p)|\Phi^+\rangle\langle\Phi^+| + \frac{p}{3}\mathbb{1} , \quad (4.29)$$

via the following detection operator:

$$W_{EB} = \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} - X \otimes X + Y \otimes Y - Z \otimes Z) . \quad (4.30)$$

The detection scheme is depicted in Fig. 4.7 (a): we prepare the two-qubit system in the maximally entangled state  $|\Phi^+\rangle$ , we then let the depolarizing channel act on qubit 1, and we finally measure the operator  $W_{EB}$  acting on both qubits 12 for different value of the noise parameter  $p$ .

If  $\langle W_{EB} \rangle < 0$ , then we are guaranteed that the depolarizing channel  $\Gamma_p$  is not EB. The theoretically calculated expectation value for the ideal Choi state

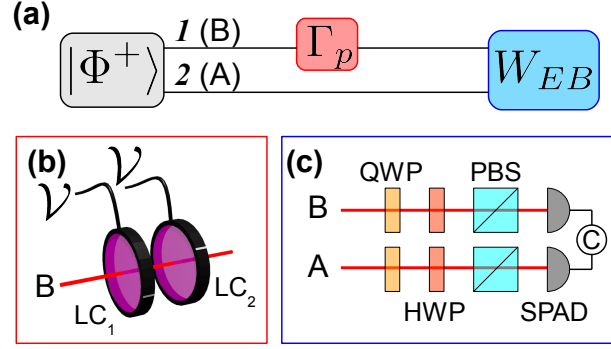


Figure 4.7: (a) Scheme for the 1-qubit depolarizing channel detection;  $|\Phi^+\rangle$ : 2-qubit maximally entangled state,  $\Gamma_p$ : 1-qubit depolarizing channel;  $W_{EB}$ : EB detection operator measurement. (b) Implementation of the 1-qubit depolarizing channel;  $LC_{1,2}$ : liquid crystal retarders with axis set at  $0^\circ$  and  $45^\circ$  respectively;  $\mathcal{V}$ : applied voltage to the LCs. (c) Polarization analysis set-up used to evaluate the operator  $W_{EB}$ ; QWP: quarter-wave plate, HWP: half-wave plate, PBS: polarizing beam-splitter, SPAD: single-photon avalanche photodiode, C: coincidence counting electronics.

is  $\langle W_{EB} \rangle = p - 1/2$ , from which we expect  $\Gamma_p$  to be non EB whenever  $p < 1/2$ . Notice that from the measured  $\langle W_{EB} \rangle$  we can also establish a lower bound on the theoretical quantity  $\mu_c(\Gamma_p)$  discussed at the end of Sec. 3.2.

**Experimental procedure:** The two-photon states used in this experiment were produced by a spontaneous parametric down conversion (SPDC) source operating on the double excitation (back and forth) of a type I,  $0.5\text{ mm}$ -long BBO crystal, that, depending on the performed experiment, allows to generate either a polarization entangled state [78], or a path-polarization hyperentangled state [79] of two photons emitted over either two or four spatial modes (see appendix D.1 for major details). The 2-photon polarization entangled state generated over two spatial modes (Fig. 4.7 (a)) was  $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_B|H\rangle_A + |V\rangle_B|V\rangle_A)$ , where  $H$  ( $V$ ) stands for the horizontal (vertical) polarization of photon  $A$  (Alice's) or  $B$  (Bob's).

We simulated a 1-qubit depolarizing channel,  $\Gamma_p$  of Eq. (3.7), acting on Bob's photon by inserting two liquid crystal retarders ( $LC_1$  and  $LC_2$ ) on the path of photon  $B$ , one having its fast axis horizontal and the other oriented at  $45^\circ$  with respect to the horizontal [76] (Fig. 4.7 (b)). Depending on the applied voltage  $\mathcal{V}$ , it is possible to change the retardation between ordinary and extraordinary polarized radiation. More precisely, by applying either  $\mathcal{V}_1$  or  $\mathcal{V}_\pi$  to a LC, it can be made to act as either a full- or a half-wave plate, respectively. Thus, by varying independently the voltage applied to  $LC_1$  and  $LC_2$  for different time intervals, we could apply the four Pauli operators to photon  $B$  with different values of the weight  $p$  (see appendix D.1).

In order to measure the detection operator  $W_{EB}$  given by Eq. (4.30) as

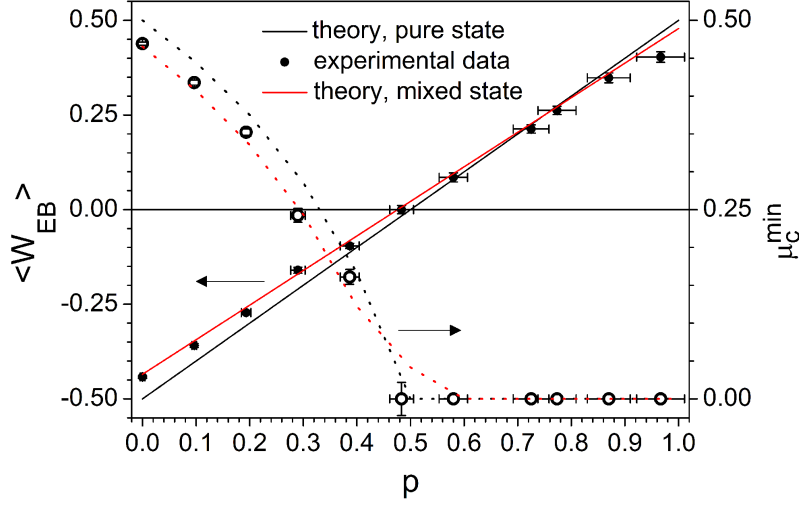


Figure 4.8: Expectation value  $\langle W_{EB} \rangle$  of the detection operator (full symbol, solid line) and minimal bound of  $\mu_c(\Gamma_p)$  (empty symbol, dotted line) as a function of the noise parameter  $p$ .

a function of the noise level, varying between the values 0 and 1, we needed to evaluate  $X^{\otimes 2}$ ,  $Y^{\otimes 2}$  and  $Z^{\otimes 2}$  for different values of  $p$ . This was done, for each choice of  $p$ , by measuring the coincidences between photons  $A$  and  $B$  in 8 different settings [80] of the polarization analysis set-up which consisted of a quarter-wave plate (QWP), a half-wave plate (HWP), a polarizing beam-splitter (PBS) and a single-photon avalanche photodiode (SPAD) (Fig. 4.7 (c)).

**Experimental results:** The detection operator we obtained is shown in Fig. 4.8, together with the theoretical behaviour for a perfectly pure state and the actual one used in the experiment. In order to compare our results with the theory, we need in fact to take into account the imperfection of the experimentally simulated Choi state. Indeed, the two-photon state produced by the SPDC source corresponds to  $|\Phi^+\rangle$  only up to a finite fidelity  $F_0 = 0.935 \pm 0.004$  (measured by performing a two-photon quantum state tomography for  $p = 0$ ). Replacing

$$|\Phi^+\rangle\langle\Phi^+| \longrightarrow \frac{4F_0 - 1}{3}|\Phi^+\rangle\langle\Phi^+| + \frac{4 - 4F_0}{3}\frac{\mathbb{1}}{4} \quad (4.31)$$

in Eq. (4.29), we can thus write the experimental Choi state as:

$$C_{\Gamma_p, \text{exp}} = \left(1 - \frac{4p}{3}\right) \frac{4F_0 - 1}{3} |\Phi^+\rangle\langle\Phi^+| + \left(\frac{p}{3} \frac{4F_0 - 1}{3} + \frac{1 - F_0}{3}\right) \mathbb{1}. \quad (4.32)$$

Notice that the experimental data are in full agreement with the theoretical value  $\langle W_{EB} \rangle$ , computed on the noisy state  $C_{\Gamma_p, \text{exp}}$  with  $F_0 = 0.935 \pm 0.004$ . The error bars on  $\langle W_{EB} \rangle$  are obtained by propagating the Poissonian uncertainties

associated with the coincidence counts and the error bars on  $p$  are estimated by considering the finite response time of the LC.

Let us notice that we indeed obtain the EB property of the channel for a value of  $p$  up to around 0.5 as expected from the theory, and, as a consequence of Eq. (3.10), the bound on  $\mu_c(\Gamma_p)$  gets trivial above this value (see Fig. 4.8).

### 4.3.2 Two-qubit separable maps

As a demonstration of the achievability of the optimal detection method for non separable maps we consider the explicit case of the CNOT gate acting on two qubits  $12$ . Following the method explained in Sec. 3.3 and already recalled in Sec. 4.1 of this chapter, the corresponding detection operator reads

$$W_{\text{CNOT}} = \frac{1}{2} \mathbb{1} - |\text{CNOT}\rangle\langle\text{CNOT}|, \quad (4.33)$$

where  $|\text{CNOT}\rangle$  is the Choi state associated to the CNOT gate (now taken with qubit  $1$  as the target and qubit  $2$  as the control, contrarily to the usual convention). The Choi state  $|\text{CNOT}\rangle$  is thus given by

$$\begin{aligned} |\text{CNOT}\rangle &= \text{CNOT}_{21} \otimes \mathbb{1}_{34} |\Phi^+\rangle_{13} |\Psi^+\rangle_{24} \\ &= \frac{1}{\sqrt{2}} (|\Phi^+\rangle_{13} |01\rangle_{24} + |\Psi^+\rangle_{13} |10\rangle_{24}), \end{aligned} \quad (4.34)$$

where  $|\Phi^+\rangle$  and  $|\Psi^+\rangle$  are maximally entangled states of the Bell basis. Notice that here we implement the above state by starting from the maximally entangled state  $|\Phi^+\rangle_{13} |\Psi^+\rangle_{24}$ , instead of  $|\Phi^+\rangle_{13} |\Phi^+\rangle_{24}$ . This choice, besides not affecting the technique, will be more convenient in the experimental realization that follows. The detection operator above can be measured by using nine different local measurement settings, see Sec. 3.3. Notice that a possible way to reduce the experimental effort is to consider the suboptimal operator

$$\begin{aligned} \tilde{W}_{\text{CNOT}} &= 3 \mathbb{1} - 2 \left[ \frac{(\mathbb{1} + \mathbb{1} X^{\otimes 3})}{2} \frac{(\mathbb{1} + X \mathbb{1} X \mathbb{1})}{2} \right. \\ &\quad \left. + \frac{(\mathbb{1} - \mathbb{1} Z \mathbb{1} Z)}{2} \frac{(\mathbb{1} + Z^{\otimes 3} \mathbb{1})}{2} \right], \end{aligned} \quad (4.35)$$

where we omitted the tensor products and from which it is clear that it requires only two measurement settings.

In this experiment we also demonstrate the robustness of the detection method in the presence of undesired dephasing noise acting on both qubits  $12$ , before and/or after the CNOT gate, as discussed in Sec. 4.2.2. The noise robustness of the operator  $\tilde{W}_{\text{CNOT}}$  with respect to dephasing noise is evaluated by the expectation value of  $\tilde{W}_{\text{CNOT}}$  given by Eq. (4.35) with respect to the state  $C_{\mathcal{M}_{D,X}}$ , the Choi state corresponding to the noisy map depicted in (4.18) with  $U_t = X$ . We would like to stress that, despite requiring only

#### 4. Map Detection: Noise Robustness and Experimental Realization

two measurement settings, the operator  $\tilde{W}_{\text{CNOT}}$  of (4.35) turns out to be as efficient as  $W_{\text{CNOT}}$  of (4.33) in the presence of dephasing noise, in the sense that it detects non separability of  $C_{\mathcal{M}_{D,X}}$  in the same range of values of the noise parameters. Indeed the two operators can be shown to fulfil  $\tilde{W}_{\text{CNOT}} = 2W_{\text{CNOT}}$  if restricted to the subspace of states spanned by  $C_{\mathcal{M}_{D,X}}$ . Therefore, in the present experiment we measure  $\tilde{W}_{\text{CNOT}}$  instead of  $W_{\text{CNOT}}$ , as this requires fewer experimental settings. Furthermore, the theoretical expectation value of  $\tilde{W}_{\text{CNOT}}$  on the noisy state  $C_{\mathcal{M}_{D,X}}$  is still given by Eq. (4.19) (multiplied by a factor two), that we report for convenience in the following:

$$\text{Tr}[\tilde{W}_{\text{CNOT}} C_{\mathcal{M}_{D,X}}] = 1 - 2[(1 - q_1)^2(1 - q_2)^2 + q_1 q_2(1 - q_1 q_2)]. \quad (4.36)$$

Recall that whenever the noise has the same strength before and after the CNOT gate ( $q_1 = q_2 = q$ ), it is always possible to detect the non separability character of the map  $\mathcal{M}_{D,X}$  for sufficiently low values of the noise parameter, namely  $q < 0.17$ .

**Experimental procedure:** For this second experiment, we used the SPDC source operating over four emission modes (see appendix D.1). Hence we prepared the 4-qubit hyperentangled state  $|\Xi\rangle = |\Phi^+\rangle_{13}|\Psi^+\rangle_{24}$  where

$$|\Phi^+\rangle_{13} = \frac{1}{\sqrt{2}}(|H\rangle_B |H\rangle_A + |V\rangle_B |V\rangle_A), \quad (4.37)$$

$$|\Psi^+\rangle_{24} = \frac{1}{\sqrt{2}}(|r\rangle_B |l\rangle_A + |l\rangle_B |r\rangle_A), \quad (4.38)$$

and  $r$  ( $l$ ) designs the right (left) path of photon  $A$  or  $B$ .

We implemented a CNOT gate on Bob's photon by inserting a half-wave plate set at  $45^\circ$  on the left path of photon  $B$ : thus the path (qubit 2) acts as the control and the polarization (qubit 1) acts as the target (Fig. 4.9 (b)). After the CNOT gate, the 4-qubit state then reads:

$$\begin{aligned} |\Xi_{\text{out}}\rangle &= \frac{1}{2}(|Hr\rangle_B |Hl\rangle_A + |Vl\rangle_B |Hr\rangle_A + |Vr\rangle_B |Vl\rangle_A + |Hl\rangle_B |Vr\rangle_A) \\ &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{13}|r\rangle_2|l\rangle_4 + |\Psi^+\rangle_{13}|l\rangle_2|r\rangle_4). \end{aligned} \quad (4.39)$$

Using the correspondence  $|H\rangle_{B,A} \leftrightarrow |0\rangle_{13}, |V\rangle_{B,A} \leftrightarrow |1\rangle_{13}$ ,  $|r\rangle_{B,A} \leftrightarrow |0\rangle_{24}$  and  $|l\rangle_{B,A} \leftrightarrow |1\rangle_{24}$ , Eq. (4.39) is equivalent to the Choi state of the CNOT channel expressed in the logical basis (4.34).

Dephasing noisy processes were simulated by acting independently on qubits 1 and 2, before and/or after the CNOT gate (Fig. 4.9 (a)) by inserting a LC with its fast axis at  $0^\circ$  with respect to the horizontal and a thin glass plate, both before and after the CNOT (Fig. 4.9 (c)). Each LC induces a phase between  $|H\rangle_B$  and  $|V\rangle_B$ , that can be set to either 0 or  $\pi$  by applying a voltage  $\mathcal{V}_1$  or  $\mathcal{V}_\pi$  respectively, thus acting either as  $\mathbb{1}$  or  $Z$  for qubit 1; each glass

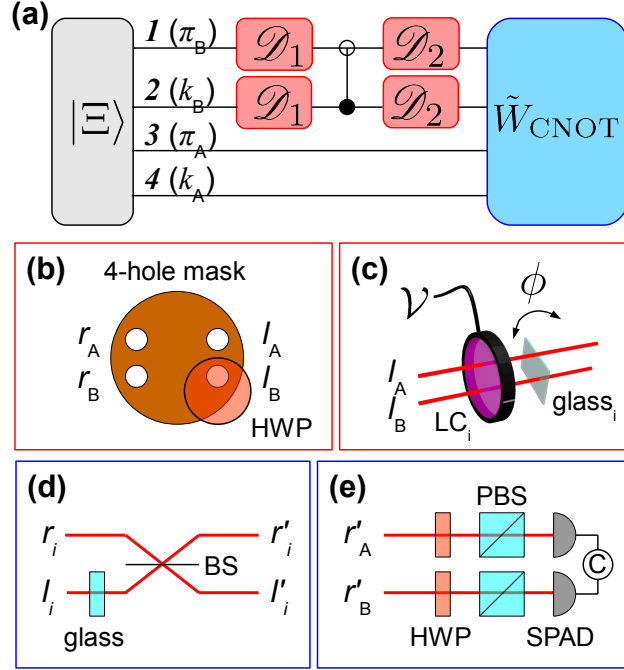


Figure 4.9: (a) Scheme for the 2-qubit CNOT channel detection in presence of dephasing noise;  $|\Xi\rangle$ : 4-qubit hyperentangled state;  $\pi_i$ : polarization qubit and  $k_i$ : path qubit, with  $i = A, B$ ;  $\mathcal{D}_{1,2}$ : independent 2-qubit dephasing channels;  $\tilde{W}_{\text{CNOT}}$ : CNOT detection operator measurement. (b) CNOT implementation: a half-wave plate (HWP) set at  $45^\circ$  flips the polarization of photon  $B$  when its path is  $l_B$ . (c) 2-qubit dephasing channel implementation;  $LC_i$ : liquid crystal retarder with its axis set at  $0^\circ$ ;  $glass_i$ : thin glass plate;  $i = 1, 2$ . (d) Path analysis set-up;  $glass$ : thin glass plate, BS: beam-splitter;  $i = A, B$ . (e) Polarization analysis set-up used in combination with (c) to evaluate the operator  $\tilde{W}_{\text{CNOT}}$ ; HWP: half-wave plate, PBS: polarizing beam-splitter, SPAD: single-photon avalanche photodiode, C: coincidence counting electronics.

plate introduces a phase  $\phi$  between  $|r\rangle_B$  and  $|l\rangle_B$ , that can be set to 0 or  $\pi$  by calibrated rotations of the plate, thus acting either as  $\mathbb{1}$  or  $Z$  for qubit 2. By varying the relative time of action of each dephaser, in a similar manner as in the 1-qubit channel experiment, we were able to vary the values of  $q_1$  and  $q_2$ .

In order to measure the operator  $\tilde{W}_{\text{CNOT}}$  (4.35) as a function of  $q_1$  and  $q_2$ , we needed to evaluate  $X^{\otimes 4}$  and  $Z^{\otimes 4}$  for several values of  $q_1$  and  $q_2$ . Thus, for each value of  $q_1$  and  $q_2$ , we measured coincidence counts between photons  $A$  and  $B$  in 32 different settings of the polarization-path analysis set-up. The polarization analysis in this case is achieved via a HWP and a PBS (Fig. 4.9 (e)) while the path analysis is done either directly sending the photons to the detectors (thus measuring  $|r\rangle$  and  $|l\rangle$ ) or passing them first through a beam-splitter and a thin glass plate (thus measuring  $|d\rangle = \frac{1}{\sqrt{2}}(|r\rangle + |l\rangle)$  and  $|a\rangle = \frac{1}{\sqrt{2}}(|r\rangle - |l\rangle)$ ) (Fig. 4.9 (d)).

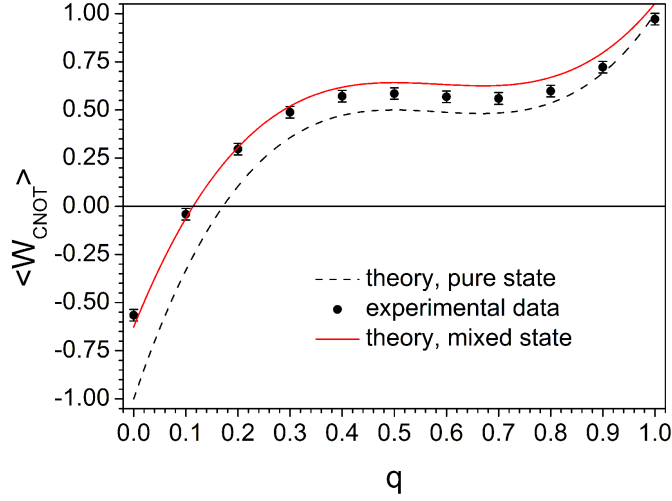


Figure 4.10: CNOT detection operator expectation value  $\langle \tilde{W}_{\text{CNOT}} \rangle$  as a function of the noise parameter  $q$ .

**Experimental results:** We obtained the values reported in Fig. 4.10 as a function of  $q_1 = q_2 = q$ . Again, to compare them properly with the theory, we must take into account the finite purity of the initial state that we prepared to simulate the Choi state of the CNOT gate. We could model the experimental Choi state of the CNOT noisy channel, given the visibilities (measured in the diagonal basis) of the polarization ( $\nu_\pi = 0.858 \pm 0.008$ ) and path ( $\nu_k = 0.904 \pm 0.004$ ) entanglement for  $q = 0$  (see appendix D.2).

As can be seen, our results are in good agreement with the theoretical calculation. Notice that the slight discrepancy remaining for large  $q$  is probably due to imperfections in the simulated dephasing channels. As expected, from these results it is evident that a low level of noise makes the CNOT to be no more an entangling gate, in particular the non separability of the map is no longer detected for  $q \geq 0.1$  in our experiment.

Eventually, in Fig.4.11 two additional measurements of  $\langle \tilde{W}_{\text{CNOT}} \rangle$  for which only  $q_1$  was varied, in the cases  $q_2 = 0$  and  $q_2 = 0.30$ , are reported. The expectation value for the imperfect initial Choi state prepared was calculated using the model described in the appendix. Here again we believe the discrepancy with the experimental data for large  $q_1$  may be due to imperfections in the simulated dephasing noise. In the case  $q_2 = 0$ , the non separability of the map is no longer detected for  $q_1 \geq 0.21$  in our experiment; while for the case  $q_2 = 0.30$ , as expected from Sec. 4.2.1, the entanglement of the CNOT gate is never detected, whatever the strength  $q_1$  of the noise before the gate.

## 4.4 Conclusions and further perspectives

In summary, we have reviewed an experimentally feasible method to detect specific properties of noisy quantum channels and we have analysed in partic-

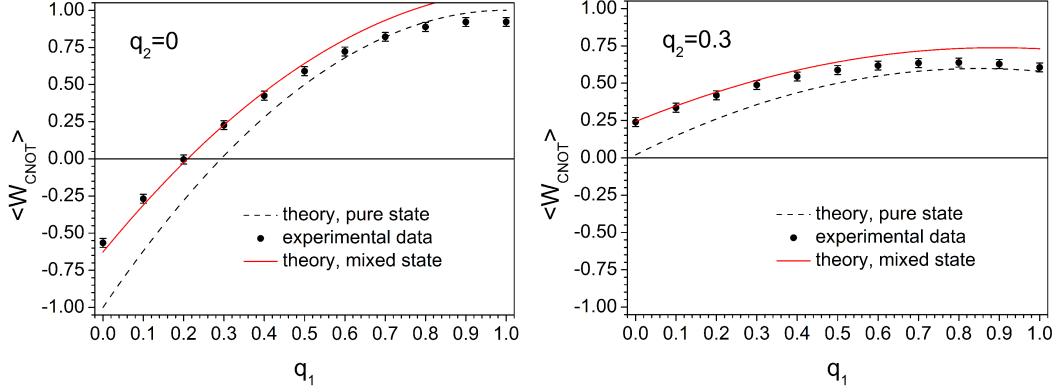


Figure 4.11: CNOT detection operator expectation value as a function of the noise parameter  $q_1$ , in two cases:  $q_2 = 0$  (left) and  $q_2 = 0.30$  (right).

ular the case of detection of non separable maps acting on two qubits. We have studied in detail the robustness of the method in the presence of noise and imperfections in the channel operation for the case of a unitary channel, considering the explicit examples of CNOT and CZ gates. We have discussed four realistic noise models, namely depolarising, dephasing, bit flip and amplitude damping noise, and derived the corresponding noise thresholds in which the method works.

The QCD method has been then tested in the cases of a single-qubit non EB channel and of a two-qubit non separable map with very good agreement between experimental measurements and theoretical predictions. We would like to stress that the presented QCD method allows to check the entanglement properties of a noisy multiqubit gate with fewer measurements than those required by full quantum process tomography [66], and could thus be a more convenient tool for routine performance checks on quantum gates.





# Chapter 5

## Quantum Cloning by Cellular Automata

Quantum cellular automata (QCAs) have attracted considerable interest in recent years [32, 33], due to their versatility in tackling several problems in quantum physics. Quantum automata describing single particles correspond to the so-called quantum random walks [81], whose probability distributions can be simulated with an optical set-up [82, 83]. Solid-state and atom-optics systems, such as spin-chains, optical lattices, or ion chains, can be viewed as implementations of QCAs, though in a Hamiltonian description. Recently QCAs have also been considered as a model of quantum field theory at the Planck scale [84, 85]. In this scenario, general coordinate transformations correspond to foliations, such as those introduced in Ref. [86] for operational structures, e.g. the digital equivalent of the relativistic boost is given by a uniform foliation over the automaton [87]. Besides the link with fundamental research, the possibility of foliations makes the QCA particularly interesting also for implementing quantum information tasks.

In this chapter we explore such a potentiality for the case of quantum cloning as a sample protocol [30]. We firstly introduce a quantum cellular automaton that achieves approximate phase-covariant cloning of qubits and optimize its performances for  $1 \rightarrow 2N$  economical cloning. We then show how the foliations can be optimized and exploited for improving the efficiency of the protocol.

### 5.1 Two fundamental preliminaries

The concepts of both phase-covariant cloning and QCAs are needed in order to understand the content of this chapter. We will thus briefly explained them in the following, mainly focusing on the basic features that are required to realize quantum cloning via QCAs.

### 5.1.1 Phase-covariant cloning

It is well known that quantum cloning of non orthogonal states violates unitarity [88] or linearity [89] of quantum theory. However, one can achieve quantum cloning approximately, for a given prior distribution over input quantum states. For uniform Haar distribution of pure states the optimal protocol has been derived in Ref. [31], whereas for equatorial states it has been given in Refs. [90, 91].

Here we consider specifically this second protocol, corresponding to clone the two-dimensional equatorial states of the form

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle). \quad (5.1)$$

The cloning is phase-covariant in the sense that its performance is independent of  $\phi$ , i.e. the fidelity is the same for all states  $|\phi\rangle$ . For certain numbers of input and output copies it was shown that the optimal fidelity can be achieved by a transformation acting only on the input and blank qubits, without extra ancillae [92, 93]. Since these transformations act only on the minimal number of qubits, they are called “economical”. The unitary operation  $U_{pcc}$  realizing the optimal  $1 \rightarrow 2$  economical phase-covariant cloning is given by [92]

$$\begin{aligned} U_{pcc} |0\rangle |0\rangle &= |0\rangle |0\rangle, \\ U_{pcc} |1\rangle |0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle |1\rangle + |1\rangle |0\rangle), \end{aligned} \quad (5.2)$$

where the first qubit is the one we want to clone, while the second is the blank qubit initialised to input state  $|0\rangle$ . In Ref. [93] the economical map performing the optimal  $N \rightarrow M$  phase-covariant cloning for equatorial states of dimension  $d$  is explicitly derived for  $M = kd + N$ , with integer  $k$ .

### 5.1.2 Quantum cellular automata

In order to analyse a QCA implementation of the economical quantum cloning, we now recall the reader some properties of QCAs we are considering here.

Our automaton is one-dimensional, and a single time-step corresponds to a unitary shift-invariant transformation achieved by two arrays of identical two-qubit gates in the two-layer Margolus scheme [32] reported in Fig. 5.1. Notice that this is the most general one-dimensional automaton with next-nearest neighbour interacting minimal cells. Due to the locality of interactions, information about a qubit cannot be transmitted faster than two-systems per time step, and this corresponds to the cell (qubit) “light-cone” made of cells that are causally connected to the first. Every event outside the cone has no chance to be influenced by what happened in the first cell, thus the quantum computation of the evolution of localized qubits is finite for finite numbers of time-steps.

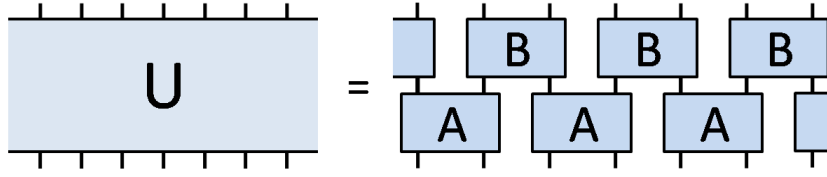


Figure 5.1: Realization of one-dimensional quantum cellular automaton with a structure composed of two layers of gates  $A$  and  $B$ . This is the most general one-dimensional automaton with next-nearest neighbour interacting minimal cells.

We now remind the concept of foliation on the gate-structure of the QCA [87]. Usually in a quantum circuit –drawn from the bottom to the top as the direction of input output– one considers all gates with the same horizontal coordinate as simultaneous transformations. A foliation on the circuit corresponds to stretching the wires (namely without changing the connections), and considering as simultaneous all the gates that lie on the same horizontal line after the stretching. Such horizontal line can be regarded as a leaf of the foliation on the circuit before the stretching transformation. Therefore, a foliation corresponds to a specific choice of simultaneity of transformations (the “events”), namely it represents an observer or a reference frame. Examples of different foliations are given in Fig. 5.2. Upon considering the quantum state at a specific leaf as the state at a given time (at the output of simultaneous gates), different foliations correspond to different state evolutions achieved with the same circuit. Therefore, in practice we can achieve a specific state belonging to one of the different evolutions, by simply cutting the circuit along a leaf, and tapping the quantum state from the resulting output wires (the operation of “stretching” wires should be achieved by remembering that by convention the wires represent identical evolutions, not “free” evolutions).

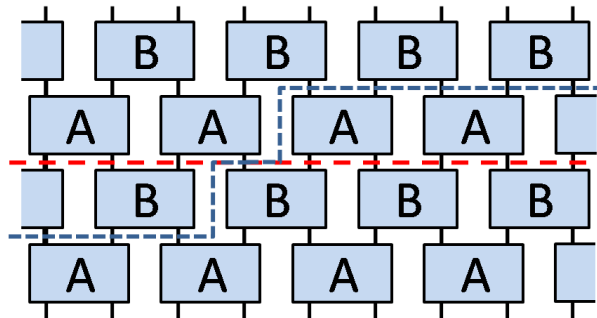


Figure 5.2: Foliations over the automaton. Two leaves of two different uniform foliations are depicted with dash-lines in different colors (the complete foliation is obtained upon repeating vertically the leaf). The systems along each leaf are taken as simultaneous. The red “cut” is usually referred to as the rest-frame foliation.

## 5.2 Phase-covariant cloning by QCAs

We now show how to perform a  $1 \rightarrow 2N$  phase-covariant cloning of the equatorial states (5.1) with a QCA of  $N$  layers, with all gates identical, performing the unitary transformation denoted by  $A$ , acting on two qubits.

Due to causality, we can restrict our treatment to the light-cone centred in the state to be cloned  $|\phi\rangle$  and initialise all blank qubits to  $|0\rangle$ , as shown in Fig. 5.3. By requiring phase-covariance for the cloning transformation, the unitary operator  $A$  must commute with every transformation of the form  $P_\chi \otimes P_\chi$ , where  $P_\chi$  is the general phase-shift operator  $P_\chi = \exp[\frac{i}{2}(\mathbb{1} - \sigma_z)\chi]$  for a single qubit, with  $\sigma_z$  the Pauli matrix along  $z$ . Therefore, we impose the condition

$$[A, P_\chi \otimes P_\chi] = 0, \quad \forall \chi. \quad (5.3)$$

This implies that the matrix  $A$  must be of the form  $A = \text{diag}(1, V, 1)$ , where  $V$  is a  $2 \times 2$  unitary matrix. Notice that the transformation  $A$  then acts non-trivially only on the subspace spanned by the two states  $\{|01\rangle, |10\rangle\}$  and it is completely specified by fixing  $V$ .

In order to derive the optimal cloning transformation based on this kind of QCA we now maximize the average single-site fidelity of the  $2N$ -qubit output state with respect to the unitary operator  $A$ . In order to achieve this, we write the initial state of  $2N$  qubits in the following compact form

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|\Omega\rangle + e^{i\phi}|N\rangle), \quad (5.4)$$

where we define  $|\Omega\rangle = |0 \dots 0\rangle$  as the “vacuum state” with all qubits in the  $|0\rangle$  state, and  $|k\rangle = |0 \dots 01_k 0 \dots 0\rangle$  as the state with the qubit up in the position  $k$ , and all other qubits in the state down. Without loss of generality in the above notation the qubit to be cloned is supposed to be placed at position  $N$  and it is initially in the state  $|\phi\rangle$ . Since  $[P_\chi \otimes P_\chi, \sum_k \sigma_{z,k}] = 0$  for all  $\chi$ , the gate  $A$  commutes with the operator  $\sum_k \sigma_{z,k}$  and thus preserves the number of qubits up. Therefore, the evolved state through each layer belongs to the Hilbert space spanned by the vacuum state and the  $2N$  states with one qubit up. The whole dynamics of the QCA can then be fully described in a Hilbert space of dimension  $2N + 1$ . The output state can thus be generally written as

$$|\Psi_{2N}\rangle = \frac{1}{\sqrt{2}}(|\Omega\rangle + e^{i\phi} \sum_{k=1}^{2N} \alpha_k |k\rangle), \quad (5.5)$$

where the amplitudes  $\alpha_k$  of the excited states depend only on the explicit form of the gate  $A$ .

The reduced density matrix  $\rho_k$  of the qubit at site  $k$  can then be straightforwardly derived from the output state (5.5) as

$$\begin{aligned} \rho_k &= \text{Tr}_{\bar{k}}[|\Psi_{2N}\rangle \langle \Psi_{2N}|] \\ &= \frac{1}{2} \left[ \left(1 + \sum_{j \neq k} |\alpha_j|^2\right) |0\rangle \langle 0| + e^{-i\phi} \alpha_k^* |0\rangle \langle 1| + e^{i\phi} \alpha_k |1\rangle \langle 0| + |\alpha_k|^2 |1\rangle \langle 1| \right], \end{aligned} \quad (5.6)$$

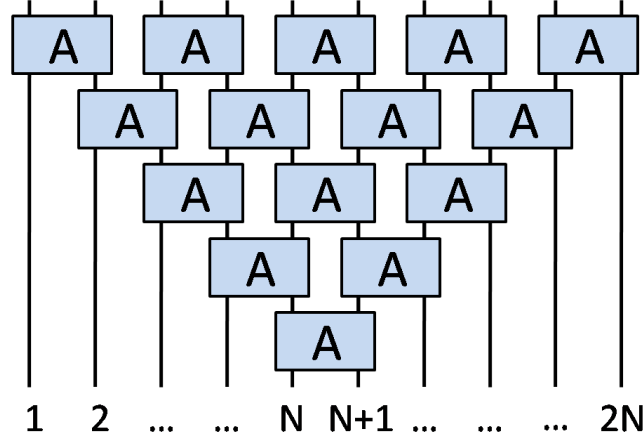


Figure 5.3: Cone of gates which contribute to the phase-covariant cloning, given the input state  $|\phi\rangle$  at site  $N$ .

where  $\text{Tr}_k$  denotes the trace on all qubits except qubit  $k$ . The local fidelity of the qubit at site  $k$  with respect to the input state  $|\phi\rangle$  then takes the simple form

$$F_k = \langle \phi | \rho_k | \phi \rangle = \frac{1}{2}(1 + \text{Re}\{\alpha_k\}). \quad (5.7)$$

As we can see,  $F_k$  depends only on the amplitude  $\alpha_k$  of the state with a single qubit up exactly at  $k$ . Since the gate  $A$  is generally not invariant under exchange of the two qubits, the fidelities at different sites are in general different. We then consider the average fidelity, namely

$$\langle F \rangle = \frac{1}{2N} \sum_{k=1}^{2N} F_k, \quad (5.8)$$

as figure of merit to evaluate the performance of the phase-covariant cloning implemented by QCAs. Notice that the whole procedure corresponds to a unitary transformation on the  $2N$ -qubit system, without introducing auxiliary systems, namely it is an economical cloning transformation.

The calculation of the amplitudes  $\alpha_k$  was performed numerically by updating at each layer the coefficients of the state (5.5). Notice that the amplitude of layer  $j$  and site  $k$  influences only the amplitudes of the subsequent layer  $j+1$  and sites either  $k-1, k$  or  $k, k+1$ , depending on whether the state  $|1\rangle$  enters in the right or left wire of  $A$ , respectively. The action of  $A$  on the qubits  $j$  and  $j+1$  can thus be written as

$$A(j, j+1) |k\rangle = \begin{cases} v_{22} |j\rangle + v_{12} |j+1\rangle & \text{if } k = j \\ v_{21} |j\rangle + v_{11} |j+1\rangle & \text{if } k = j+1 \\ |k\rangle & \text{otherwise,} \end{cases} \quad (5.9)$$

where  $v_{ij}$  are the entries of the operator  $V$  in the basis  $\{|01\rangle, |10\rangle\}$ . Notice that the vacuum state  $|\Omega\rangle$  is invariant under the action of  $A$ . The iteration of Eq. (5.9) for each layer leads to the amplitudes of the output state (5.5).

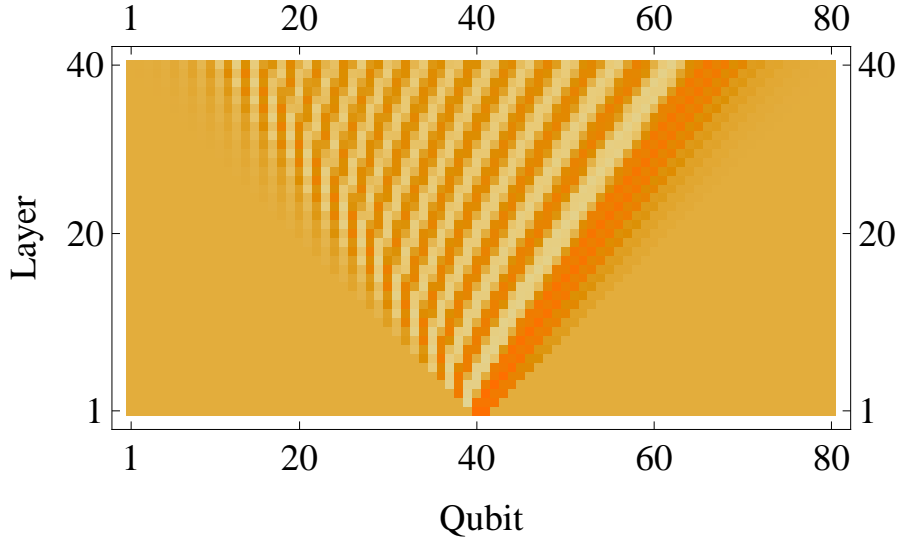


Figure 5.4: Chromatic map of the local fidelities in terms of the considered qubit and the layer. The orange colour is brighter for increasing local fidelity. The simulation involves a number of layers  $N = 40$ , while the total number of qubits is  $2N$ , since it doubles at each layer.

### 5.2.1 Performances in the rest frame

As a first explicit example we consider a QCA employing the optimal  $1 \rightarrow 2$  phase-covariant cloning (5.2). In this case the gate  $A$  must implement the unitary transformation (5.2). The non-trivial part  $V$  of gate  $A$  can then be chosen to be

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad (5.10)$$

where all coefficients are real. The corresponding local fidelities at every layer are reported in Fig. 5.4. As we can see, the figure exhibits fringes of light and dark colour. Moreover, the light-cone defined by causality can be clearly seen: outside this cone no information about the initial state can arrive, thus every system has the same fidelity of  $1/2$ . Notice that there is a sort of line, approaching the right top corner, along which the fidelity is quite high. This is because the  $1 \rightarrow 2$  phase-covariant cloning is optimised with the blank qubit initialised to the state  $|0\rangle$ . Regarding the local fidelities of the final states, they are in general quite different from each other, and can vary very quickly even between two neighbouring qubits. The average fidelity is reported in Fig. 5.5 as a function of the number of layers. Notice that the average fidelity of the optimal economical phase-covariant quantum cloning (without the constraint of automaton structure) approaches the value  $3/4$  for a large number of output copies [91].

In order to improve the average fidelity we have then maximized it with respect to the four parameters defining the unitary operator  $V$ . Numerical

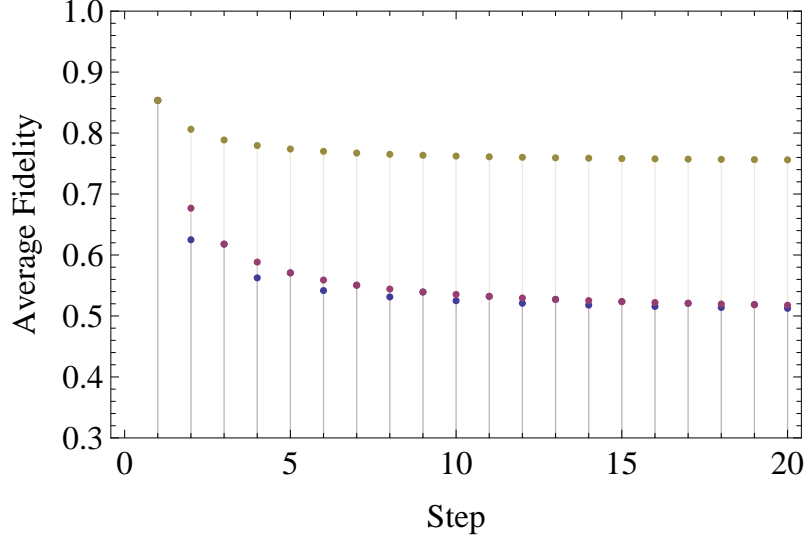


Figure 5.5: The average  $1 \rightarrow 2N$  phase-covariant cloning fidelity achieved by the QCA in the rest frame (see Fig. 5.2). Comparison with the optimal economical phase-covariant cloning in Ref. [91]. The purple dots represents the QCA cloning optimized over the unitary gate  $A$ . The blue dots correspond to the use of gate  $A$  achieving the optimal  $1 \rightarrow 2$  cloning  $U_{pcc}$  in Eq. (5.2). The yellow dots represent the unrestricted optimal economical cloning.

results achieved up to  $N = 20$  show that the optimal cloning performed in this case is not much better than the one given by the iteration of (5.10). Eventually, the latter turns out to be outperformed only when the number of layers composing the automaton is even, as shown in Fig. 5.5.

Further numerical results show that no gain can be achieved if the automaton is composed of layers of two different gates  $A$  and  $B$ . Actually, in this case it surprisingly turns out that the optimal choice corresponds to  $B = A$ , namely we do not exceed the average fidelity obtained by employing a single type of gate. As a result, since all one-dimensional QCA with next-nearest neighbour interacting cells with two qubits can be implemented by a two-layered structure, we have then derived the optimal phase-covariant cloning transformation achievable by the minimal one-dimensional QCA.

### 5.2.2 Performances exploiting different foliations

We now show that the average fidelity in the case of a single-gate automaton can be improved by considering different foliations.

Suppose that we are given a fixed number  $M$  of identical gates  $A$  to implement a QCA. We are then allowed to place the gates in any way such that the causal structure of the considered automaton is not violated. Which is the configuration, i.e. the foliation, that performs the optimal phase-covariant



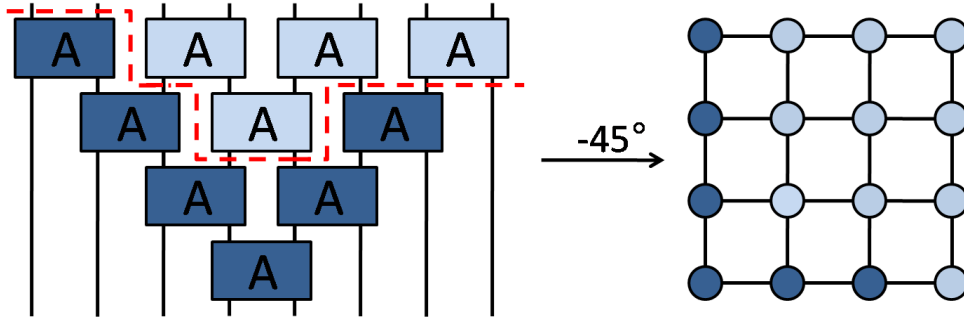


Figure 5.6: Illustration of the classification of foliations. A possible foliation with  $M = 6$  gates is given. From the correspondence between the gates lying under the “cut” and the rotated dots on the right, we identify this foliation with the partition  $\{4, 1, 1\}$ .

cloning for fixed  $M$ ? In this framework we have to maximize not only over the parameters that define  $V$  but also over all possible foliations. Thus, the  $M$  fixed gates play the role of computational resources, and the optimality is then defined in terms of both the parameters characterising the single gate  $A$  and the disposition of the gates in the network.

As a first example, suppose that we are given  $M = 3$  gates. In this case there are 3 inequivalent foliations: one for the rest frame (see Fig. 5.2), and two along the straight lines defining the light-cone. As expected, for increasing  $M$  the counting of foliations becomes more complicated and the problem is how to choose and efficiently investigate each possible foliation. It turns out that the problem of identifying all possible foliations of a QCA of the form illustrated in Fig. 5.3 for a fixed number of gates  $M$  is related to the partitions of the integer number  $M$  itself (by partition we mean a way of writing  $M$  as a sum of positive integers, a well known concept in number theory [94]). Two sums that differ only in the order of their addends are considered to be the same partition. For instance the partitions of  $M = 3$  are exactly 3 and given by  $\{3\}$ ,  $\{2, 1\}$ , and  $\{1, 1, 1\}$ , while the partitions of  $M = 6$ , corresponding to a 3-layer setting in the rest frame, are 11 and given by  $\{6\}$ ,  $\{5, 1\}$ ,  $\{4, 2\}$ ,  $\{4, 1, 1\}$ ,  $\{3, 3\}$ ,  $\{3, 2, 1\}$ ,  $\{3, 1, 1, 1\}$ ,  $\{2, 2, 2\}$ ,  $\{2, 2, 1, 1\}$ ,  $\{2, 1, 1, 1, 1\}$ , and  $\{1, 1, 1, 1, 1, 1\}$ . The link between foliations and partitions is illustrated in Fig. 5.6, which shows how partitions can be exploited to identify foliations. For a fixed number of gates  $M$  the number of foliations is then automatically fixed and each foliation corresponds to a single partition. The correspondence is obtained as follows: each addend represents the number of gates along parallel diagonal lines, starting from the vertex of the light-cone, as shown in Fig. 5.6 for the particular case of  $M = 6$ .

Based on this correspondence, we can investigate the performance of the phase-covariant cloning as follows. For any fixed foliation, we first maximize the average fidelity with respect to the four parameters of the unitary  $V$ , defining the gate  $A$ . Then we choose the highest average fidelity that we have

$M(\text{Layers})$	$\langle F_{\text{rest}} \rangle$	$\langle F \rangle$	Optimal foliation
1(1)	0.853	0.853	{1}
3(2)	0.676	0.693	{3}
6(3)	0.617	0.679	{2, 2, 2}
10(4)	0.588	0.670	{4, 3, 3}
15(5)	0.570	0.653	{4, 4, 4, 3}
21(6)	0.558	0.614	{4, 3, 2, 2, 2, 2, 2, 2}
28(7)	0.550	0.603	{6, 6, 6, 5, 5}

Table 5.1: Results of the maximization over foliations up to  $M = 28$  corresponding to QCAs composed of up to 7 layers.

obtained by varying the foliation. We worked out this procedure numerically for  $M = 1, 3, 6, 10, 15, 21, 28$ , i.e. the number of gates composing the QCA with  $N = 1, 2, 3, 4, 5, 6, 7$  layers, respectively. Our results are shown in Table 5.1, where the maximization in the rest frame is also reported for comparison. As we can see, exploiting different foliations leads to a substantial improvement of the average fidelity.

### 5.3 Summary of results

In this chapter we have introduced a way of achieving quantum cloning through QCAs. We have derived the optimal automaton achieving economical phase-covariant cloning for qubits. We have shown how the fidelity of cloning can be improved by varying the foliation over the QCA, with fixed total number of gates used.

By developing an efficient method to identify and classify foliations by means of number theory, we have thus optimised the performance of the QCA phase-covariant cloning for a given fixed number of identical gates, and obtained in this way the most efficient foliation.



# Conclusions

In this work we have mainly presented several results related either to the quantum states that are employed in quantum algorithms, and to the quantum channel detection method, i.e. a theoretical technique suitable to point out specific properties of quantum channels.

With regards to the former, we have connected real equally weighted states to hypergraph states, a new class of quantum states defined according to underlying mathematical hypergraphs. Some meaningful properties of the concerned states, as e.g. entanglement, become then more accessible and much easier to investigate. It is worth mentioning that the study of entanglement content of such states is of great importance, as it is a possible way to access the origin of the great computational power of quantum physics. Furthermore, due to their simple mathematical structure, real equally weighted states are often employed in other quantum protocols. Thus, a deeper understanding of these states might shed new light on their role in other branches of quantum information. In order to understand the role of entanglement in quantum computing, we have also calculated the dynamics of entanglement along the Grover algorithm, showing that is scale invariant and never vanishing. Moreover, several well-known criteria, that provide an efficient classical simulation of quantum computation, have been applied in the Grover case. However, none of them has turned out to be successful, suggesting that something really quantum could be effectively exploited by Grover's algorithm.

On the other hand, a theoretical technique to detect quantum channels has been basically developed in order to simplify the routine checks on experimentally realized quantum gates. Indeed, the method can be applied whenever some a priori knowledge about the form of the channel is available, as it is very often the case in a laboratory. The method is able to point out some specific properties of interest by avoiding full quantum process tomography, a technique that requires a large number of measurement settings and is not convenient if one is interested just in a single property of the channel under consideration. In other words, despite being more informative than quantum channel detection, the quantum process tomography usually provides much information that is practically not needed. The quantum channel detection

method overcomes this fact, providing knowledge about only the properties of interest. In addition, the proposed method can be implemented with nowadays technology, leading to a ready-to-use protocol to check performances of experimentally realized quantum gates.

At last, we have shown how to realize phase-covariant quantum cloning via quantum cellular automata. Even though it does not fit into the two main topics faced in this work, the achieved result should be regarded as a significant example showing how to perform a very well-known quantum task, such as cloning, by using the recently spread field of quantum cellular automata. We would like to stress that, since quantum cellular automata can be seen as networks of local gates, the presented task can be eventually interpreted as the realization of quantum cloning by a very simple quantum network.

# Appendix A

## A.1 Group structure of the generalized stabilizer operators

We now prove that the operators  $\{K_i\}_{i=1,2,\dots,n}$  defined in Eq. (1.14) generate an Abelian group. The group properties follow immediately: the closure is given by construction, the associativity by the matrix algebra, the identity and the inverse belong to the set since  $K_i^2 = \mathbb{1}$  and  $K_i = K_i^\dagger$ , respectively.

On the other hand, the commutativity can be proved as follows. Suppose we are given  $K_i$  and  $K_j$  with  $i \neq j$ , otherwise everything trivialises. Since the concept of neighbourhood is symmetric we can keep  $K_i$  fixed and see what happens for different  $K_j$ . If  $j$  is not in  $N(i)$  then the stabilizer operators trivially commute. Therefore, the only situations we have to check is when  $j \in N(i)$ , namely when some of the  $CZ$  gates acting on  $N(i)$  in the definition of  $K_i$  involve also the qubit  $j$ . Each of these gates takes the form  $C^k Z_{ji_1 i_2 \dots i_{k-1}}$  (with  $k$  arbitrary) and generally does not commute with  $X_j$  defining  $K_j$ .

It is nevertheless easy to see that, in order to prove that  $[K_i, K_j] = 0$ , it is sufficient to show that

$$[(X_i \otimes C^k Z_{ji_1 i_2 \dots i_{k-1}}), (C^k Z_{ii_1 i_2 \dots i_{k-1}} \otimes X_j)] = 0, \quad (\text{A.1})$$

for any number of qubits  $k - 1$  and vertices  $i_1 i_2 \dots i_{k-1}$ . This is because we can think to commute the two operators  $K_i$  and  $K_j$  by following a step-by-step procedure consisting in swapping each term  $(X_i \otimes C^k Z_{ji_1 i_2 \dots i_{k-1}})$  of  $K_i$  with the corresponding term  $(C^k Z_{ii_1 i_2 \dots i_{k-1}} \otimes X_j)$  of  $K_j$ .

In order to prove Eq. (A.1), we rewrite the general controlled  $Z$  gate acting on  $k$  qubits as

$$C^k Z_{ji_1 i_2 \dots i_{k-1}} = \mathbb{1}_j \otimes (\mathbb{1} - P)_{i_1 i_2 \dots i_{k-1}} + Z_j \otimes P_{i_1 i_2 \dots i_{k-1}}, \quad (\text{A.2})$$

where  $P_{i_1 i_2 \dots i_{k-1}} = |11\dots 1\rangle_{i_1 i_2 \dots i_{k-1}} \langle 11\dots 1|$ . Then, by exploiting the anti-com-

mutativity of Pauli matrices, it follows that

$$\begin{aligned}
(X_i \otimes C^k Z_{j i_1 i_2 \dots i_{k-1}})(C^k Z_{i i_1 i_2 \dots i_{k-1}} \otimes X_j) &= \\
&= (X_i \otimes \mathbb{1}_j \otimes (\mathbb{1} - P)_{i_1 i_2 \dots i_{k-1}} + X_i \otimes Z_j \otimes P_{i_1 i_2 \dots i_{k-1}}) \\
&\times (\mathbb{1}_i \otimes X_j \otimes (\mathbb{1} - P)_{i_1 i_2 \dots i_{k-1}} + Z_i \otimes X_j \otimes P_{i_1 i_2 \dots i_{k-1}}) \\
&= X_i \otimes X_j \otimes (\mathbb{1} - P)_{i_1 i_2 \dots i_{k-1}} + X_i Z_i \otimes Z_j X_j \otimes P_{i_1 i_2 \dots i_{k-1}} \\
&= X_i \otimes X_j \otimes (\mathbb{1} - P)_{i_1 i_2 \dots i_{k-1}} + Z_i X_i \otimes X_j Z_j \otimes P_{i_1 i_2 \dots i_{k-1}} \\
&= (C^k Z_{i i_1 i_2 \dots i_{k-1}} \otimes X_j)(X_i \otimes C^k Z_{j i_1 i_2 \dots i_{k-1}}). \tag{A.3}
\end{aligned}$$

Thus, since the commutativity relation stated in Eq. (A.1) holds for any  $k - 1$  and qubits  $i_1 i_2 \dots i_{k-1}$ , the commutativity of any two stabilizers defined by (1.14) finally follows.

## A.2 Equivalence of the circuit definition and the stabilizers description

In order to prove that the two definitions stated in the main article are equivalent we essentially follow Ref. [35]. The proof is by induction on the number of hyperedges. The case with no hyperedges is trivially stabilized by the Pauli matrices  $\{X_1, X_2, \dots, X_n\}$ , since the corresponding graph state is given by  $|+\rangle^{\otimes n}$ . Suppose now a general hypergraph state  $|g_{\leq n}\rangle$ , corresponding to the hypergraph  $g_{\leq n}$ , is stabilized by  $K_i$  as defined in (1.14), namely  $K_i |g_{\leq n}\rangle = |g_{\leq n}\rangle$ . We want to show that if we apply  $C^k Z_{i_1 i_2 \dots i_k}$  to  $|g_{\leq n}\rangle$ , the new hypergraph state  $|g'_{\leq n}\rangle = C^k Z_{i_1 i_2 \dots i_k} |g_{\leq n}\rangle$  is stabilized by a new stabilizer generated by  $K'_i$ , derived from the hypergraph  $g'_{\leq n}$  where the  $k$ -hyperedge  $\{i_1, i_2, \dots, i_k\}$  is added (or removed). Namely we want to prove that  $K'_i |g'_{\leq n}\rangle = |g'_{\leq n}\rangle$ , where  $K'_i$  is defined according to (1.14) for the new hypergraph  $g'_{\leq n}$ .

If we consider  $i \neq i_1, i_2, \dots, i_k$  then by definition we have  $K'_i = K_i$  and, since  $[K_i, C^k Z_{i_1 i_2 \dots i_k}] = 0$ , the following holds

$$K'_i |g'_{\leq n}\rangle = |g'_{\leq n}\rangle \text{ for } i \neq i_1, i_2, \dots, i_k. \tag{A.4}$$

So, as for the proof regarding the commutativity of the stabilizer group, we need to focus only on the operators  $\{K'_{i_1}, K'_{i_2}, \dots, K'_{i_k}\}$ , since the others are not affected by the action of  $C^k Z_{i_1 i_2 \dots i_k}$ . Keeping in mind the decomposition (A.2) of  $C^k Z_{i_1 i_2 \dots i_k}$ , it is then easy to show that for every  $i = i_1, i_2, \dots, i_k$  the following relation holds

$$C^k Z_{i_1 i_2 \dots i_k} K_i C^k Z_{i_1 i_2 \dots i_k} = C^{k-1} Z_{i_2 \dots i_k} K_i = K'_i \text{ for } i = i_1, i_2, \dots, i_k. \tag{A.5}$$

Therefore, by exploiting the equation above, we can easily show that the hypergraph state  $|g'_{\leq n}\rangle$  is eigenstate of  $K'_i$  with eigenvalue one for vertices  $i = i_1, i_2, \dots, i_k$ . Hence, it follows that the hypergraph state  $|g'_{\leq n}\rangle$  is stabilized by any  $K'_i$  with  $i = i_1, i_2, \dots, i_n$ , which are the correlation operators that can be defined according to the hypergraph  $g'_{\leq n}$ .

### A.3 Inequivalence of $k$ -uniform hypergraphs under the local Pauli group

Here we prove that every  $k$ -uniform hypergraph state cannot be transformed to any other  $k'$ -uniform hypergraph with  $k \neq k'$ , by the only action of local Pauli operators, namely  $X$ ,  $Y$  and  $Z$ .

Let us rewrite a general hypergraph state in the more convenient form

$$|g_{\leq n}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} c_{\alpha_l^x} |x\rangle, \quad (\text{A.6})$$

where  $\alpha_l^x$  denotes the set of cardinality  $l$  of subsystems of the state  $|x\rangle$  that are in the state  $|1\rangle$ . In other words, given the state  $|x\rangle$ ,  $\alpha_l^x$  represents the set of indices corresponding to qubits where the excitations are. Then, having in mind that a general  $k$ -uniform hypergraph can be created from  $|+\rangle^{\otimes n}$  using  $\prod_j C^k Z_{\alpha_k^j}$  ( $\alpha_k^j$  are index sets of cardinality  $k$  referring to the vertices on which the  $C^k Z$  operations act, for a given hyperedge  $j$ ), it is easy to see that for any  $k$ -uniform state there is at least one  $c_{\alpha_k}$  negative (condition C1) and all  $c_{\alpha_{k'}}$  with  $k' < k$  are positive (condition C2).

In the following we prove that, starting from a  $k' < k$ -uniform hypergraph state, it is not possible to transform it into a  $k$ -uniform one by only using local  $X$  and  $Z$ . Notice that, as  $Y = iXZ$ , the  $Y$  operations are already considered. Furthermore, since  $X$  and  $Z$  anti-commute, it is not restrictive to apply always  $Z$  before  $X$ . As a result the two following cases describe the most general strategy we could apply.

*Case 1)* We just use any  $k' < k$  controlled  $Z$  operations (which includes local  $Z$ 's when  $k' = 1$ ). This nevertheless fails always because to make  $c_{\alpha_k}$  negative we generate at least one  $c_{\alpha_{k'}}$  with  $k' < k$  which is negative as well, which contradicts C2.

*Case 2)* We apply arbitrary  $k' < k$  controlled  $Z$  operations and then include any number of  $X$  gates anywhere. We now show that this procedure will fail

$N_{\beta_l \setminus \alpha_k}$	$N_{cr}$	$N_{\beta_l \cap \alpha_k}$	$N_{\alpha_k \setminus \beta_l}$	$N_{\gamma_{l'}}$
odd	odd	odd	even	odd (1)
			odd	even (2)
even	even	odd	even	even (3)
			odd	odd (4)
even	odd	even	even	even (5)
			odd	odd (6)
odd	even	even	even	odd (7)
			odd	even (8)

Table A.1: All possible cases for index sets - for an explanation, see main text.



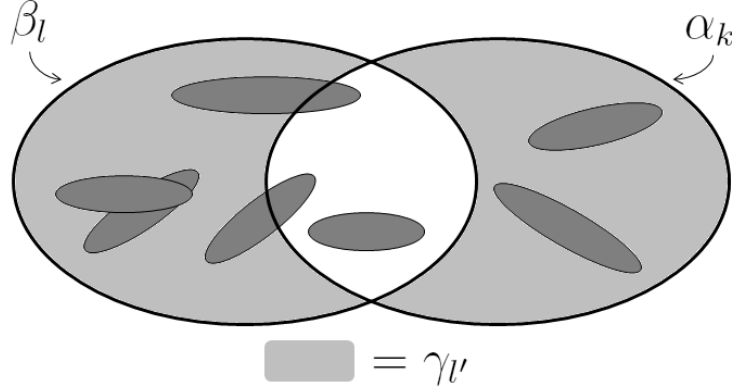


Figure A.1: Drawing showing an example for possible index sets. Each dark grey circle represents a set  $\alpha_{k'}$ . In this case  $N_{\beta_l \setminus \alpha_k} = 2$ ,  $N_{cr} = 2$ ,  $N_{\beta_l \cap \alpha_k} = 1$ ,  $N_{\alpha_k \setminus \beta_l} = 2$  and  $N_{\gamma_{l'}} = 4$ . This is an example of case (3) in Table A.1. Notice that we do not take into account the case where subsets  $\alpha_{k'}$  cross the border between the set  $\alpha_k \setminus \beta_l$  and the intersection, since it is easy to see that this case never affects our counting.

again. Let us denote as  $c_{\beta_l}$  the coefficient that will afterwards be transformed to the negative coefficient  $c_{\alpha_k}$  ( $l$  is of course arbitrary). We then need to apply  $X$  in  $\gamma_{l'} \equiv (\alpha_k \cup \beta_l) \setminus (\alpha_k \cap \beta_l)$  (such that  $c_{\beta_l} \rightarrow c_{\alpha_k}$  and C1 holds). Now, since the action of  $X$ 's cannot change the sign of the coefficient  $c_{\beta_l}$ , the number of  $C^{k'} Z_{\alpha_{k'}}$  operations we apply in the set  $\beta_l$  must be odd (thus the number of different subsets  $\alpha_{k'}$  must be odd as well). Let us denote this number as  $N_{\beta_l}$ , and in the following  $N_S$  will always denote the number of sets  $\alpha_{k'}$  (coming from  $C^{k'} Z_{\alpha_{k'}}$  operations) included in the general set of indices  $S$ . We can then distinguish four different cases that may happen, summarised in Table A.1.

By  $N_{cr}$  we mean the subsets  $\alpha_{k'}$  that lie across the border of the set  $\beta_l \setminus \alpha_k$  and the intersection  $\beta_l \cap \alpha_k$  (see Fig. A.1 for a comprehensible explanation). Notice that  $N_{\beta_l} = N_{\beta_l \setminus \alpha_k} + N_{cr} + N_{\beta_l \cap \alpha_k}$  must be odd from the hypothesis, while the number of sets  $\alpha_{k'}$  in  $\alpha_k \setminus \beta_l$ , namely  $N_{\alpha_k \setminus \beta_l}$ , is instead not determined, and might be either odd or even. Notice that the number of subsets  $\alpha_{k'}$  in  $\gamma_{l'}$  is given by  $N_{\gamma_{l'}} = N_{\beta_l \setminus \alpha_k} + N_{\alpha_k \setminus \beta_l}$ .

For the cases (1) – (4) – (6) – (7) the contradiction to C2 can be found by realizing that  $c_{\gamma_{l'}} = -1$  (since  $N_{\gamma_{l'}}$  is odd). This coefficient will be mapped into  $c_{\emptyset} = -1$  (the coefficient of the state with all zeros) by the action of  $X_{\gamma_{l'}}$ , and thus contradicting C2.

For the cases (2) – (3) the contradiction to C2 is given by  $c_{\gamma_{l'} \cup (\alpha_{k'} \in \beta_l \cap \alpha_k)} = -1$  (since  $N_{\gamma_{l'}} + N_{\beta_l \cap \alpha_k}$  is odd), which becomes  $c_{(\alpha_{k'} \in \beta_l \cap \alpha_k)} = -1$  after  $X_{\gamma_{l'}}$ . By  $\gamma_{l'} \cup (\alpha_{k'} \in \beta_l \cap \alpha_k)$  we mean the union between the set  $\gamma_{l'}$  and the sets  $\alpha_{k'}$  which belong to the intersection  $\beta_l \cap \alpha_k$ .

For the case (8) the contradiction to C2 is  $c_{\gamma_{l'} \setminus (\alpha_{k'} \in \alpha_k \setminus \beta_l)} = -1$ , since this coefficient is mapped by  $X_{\gamma_{l'}}$  into  $c_{(\alpha_{k'} \in \alpha_k \setminus \beta_l)} = -1$ . By  $\gamma_{l'} \setminus (\alpha_{k'} \in \alpha_k \setminus \beta_l)$  we mean the difference between the set  $\gamma_{l'}$  and the sets  $\alpha_{k'}$  which belong to the

set given by  $\alpha_k \setminus \beta_l$ .

Regarding the case (5), since  $N_{cr}$  is odd we can always find a subset  $\theta_t$  in the intersection  $\beta_l \cap \alpha_k$  with cardinality  $t < k$  such that the coefficient  $c_{(\beta_l \setminus \alpha_k) \cup \theta_t} = -1$ . Therefore, when we apply  $X_{\gamma_{l'}}$  this is mapped into  $c_{(\alpha_k \setminus \beta_l) \cup \theta_t} = -1$  which clearly shows a contradiction to C2 since  $(\alpha_k \setminus \beta_l) \cup \theta_t$  is a subset of  $\alpha_k$  with cardinality strictly smaller than  $k$ .



# Appendix B

## B.1 Asymptotic limit of the GME $E_n$

We now calculate the GME  $E_n$  when a single solution is concerned, i.e.  $M = 1$ , in the asymptotic limit of a large number of qubits. In order to do so, we focus on the maximal overlap that defines  $E_n$  in Eq. (2.8), namely

$$|\dots| = \frac{\cos \theta_k}{\sqrt{2^n - 1}} \left[ \left( \cos \frac{\alpha}{2} + \sin \frac{\alpha}{2} \right)^n - \sin^n \frac{\alpha}{2} \right] + \sin \theta_k \sin^n \frac{\alpha}{2}. \quad (\text{B.1})$$

Let us study the asymptotic behaviour of the above expression as  $n \gg 1$  before performing the maximization over the parameter  $\alpha$ . Remember that  $\alpha \in [0, \pi]$ , thus it is convenient to consider two cases: either  $\alpha/2 = \pi/2$  or  $\alpha/2 < \pi/2$ . Notice that in this way, we cover all possible values of  $\alpha$ , independently of the optimal value of  $\alpha$  that maximizes the overlap.

*Case  $\alpha/2 = \pi/2$*  It is trivial to show that the overlap (B.1) reduces to

$$\lim_{n \gg 1} |\dots| = \sin \theta_k. \quad (\text{B.2})$$

*Case  $\alpha/2 < \pi/2$*  In the limit  $n \gg 1$ , all terms depending only on  $\sin^n \frac{\alpha}{2}$  disappear and we have

$$\lim_{n \gg 1} |\dots| = \lim_{n \gg 1} \cos \theta_k \left( \frac{1+t}{\sqrt{2(1+t^2)}} \right)^n, \quad (\text{B.3})$$

where we have introduced the tangent  $t = \tan \alpha/2$ . Notice that the argument of the  $n$ -th power, i.e.  $\frac{1+t}{\sqrt{2(1+t^2)}}$ , is never strictly greater than 1, otherwise the overlap would become infinite in the asymptotic limit  $n \gg 1$ . Thus, considering  $n \gg 1$ , we are left with only two possibilities: either

$$\lim_{n \gg 1} |\dots| = 0, \quad (\text{B.4})$$

if the term in round brackets is strictly smaller than 1, or

$$\lim_{n \gg 1} |\dots| = \cos \theta_k, \quad (\text{B.5})$$

if the term in round brackets is exactly 1.

Therefore, the asymptotic limit forces the overlap to take only three possible different values, which are either  $\sin \theta_k$ ,  $\cos \theta_k$  or 0. The maximization of the overlap can then only converge to one of these three options, eventually providing the GME  $E_n$  in the asymptotic limit  $n \gg 1$ .

The case of two symmetric solutions, i.e.  $M = 2$ , can be studied exactly in the same way as the previous case with a single solution. Now the overlap defining  $E_n$  in Eq. (2.14) reads

$$|\dots| = \frac{\cos \theta_k}{\sqrt{2^n - 2}} \left[ \left( \cos \frac{\alpha}{2} + \sin \frac{\alpha}{2} \right)^n - \left( \cos^n \frac{\alpha}{2} + \sin^n \frac{\alpha}{2} \right) \right] + \frac{\sin \theta_k}{\sqrt{2}} \left( \cos^n \frac{\alpha}{2} + \sin^n \frac{\alpha}{2} \right), \quad (\text{B.6})$$

and we have to consider three different cases,  $\alpha/2 = 0$ ,  $\alpha/2 = \pi/2$  and  $0 < \alpha/2 < \pi/2$ .

*Case  $\alpha/2 = 0$* ) We straightforwardly get

$$\lim_{n \gg 1} |\dots| = \frac{\sin \theta_k}{\sqrt{2}}. \quad (\text{B.7})$$

*Case  $\alpha/2 = \pi/2$* ) We again obtain

$$\lim_{n \gg 1} |\dots| = \frac{\sin \theta_k}{\sqrt{2}}. \quad (\text{B.8})$$

*Case  $0 < \alpha/2 < \pi/2$* ) Following the same approach developed in the case of a single solution, we notice that the overlap for two solutions can be either 0 or  $\cos \theta_k$ .

Therefore, the GME  $E_2$  for two symmetric solutions in the asymptotic limit  $n \gg 1$  follows trivially, since the maximum of the overlap is restricted to be either  $\sin \theta_k / \sqrt{2}$ ,  $\cos \theta_k$  or 0.

## B.2 Calculation of the GME $E_2$

Here we show how to compute the maximal eigenvalue of the reduced density operator  $\rho_P = \text{Tr}_Q[|\psi_{k,M=1}\rangle \langle \psi_{k,M=1}|]$  of the states  $|\psi_{k,M=1}\rangle$  with a single solution in terms of the number  $m$  of qubits that compose the bipartition  $P$ . Recall that the reduced state  $\rho_P$  is given by the following  $2^m \times 2^m$  matrix

$$\rho_P = \begin{pmatrix} a & \dots & a & b \\ \vdots & \ddots & \vdots & \vdots \\ a & \dots & a & b \\ b & \dots & b & c \end{pmatrix}, \quad (\text{B.9})$$

where  $a = 2^{n-m}A^2$ ,  $b = a - A(A - B)$ , and  $c = a - A^2 + B^2$ , with  $A = \cos \theta_k / \sqrt{2^n - 1}$  and  $B = \sin \theta_k$ . Notice that  $\rho_P$  has rank two, and then we expect only two strictly positive eigenvalues.

In order to calculate the two non-vanishing eigenvalues of  $\rho_P$  we aim at reducing the matrix  $\rho_P - \lambda \mathbf{1}$ , defining the secular equation, to a lower triangular matrix as follows. We substitute the 1-st column for the difference between the 1-st and the 2-nd column, and then we do the same with the 1-st row. We do the same step by step for all the first  $(2^m - 2)$  columns and rows, so that we arrive at following matrix

$$\begin{pmatrix} -2\lambda & \lambda & & & 0 \\ \lambda & \ddots & \ddots & & \\ & \ddots & -2\lambda & \lambda & \\ & & \lambda & a - \lambda & b \\ 0 & & & b & c - \lambda \end{pmatrix}. \quad (\text{B.10})$$

In order to make the above matrix lower triangular, we now multiply the 2-nd column by 2, and sum it to the 1-st column. At last, we substitute the 2-nd column for the previously obtain result. Next, we do the same for the 3-rd column, but now we multiply by 3, instead of by 2 and again we substitute. Generally, we continue multiplying the  $j$ -th column by  $j$  and summing it to the  $j - 1$ -th column previously found, and substituting the  $j$ -th column for the obtained result. Following this procedure, it is straightforward to show that the two non-vanishing eigenvalues are given by the roots of the following equation

$$\lambda^2 - [a(2^m - 1) + c]\lambda + (2^m - 1)(ac - b^2) = 0. \quad (\text{B.11})$$

Therefore, fixed the bipartition  $m$ , the maximal eigenvalue reads

$$\lambda_{max} = \frac{1}{2} + \frac{1}{2} [1 - 4(2^m - 1)(2^{n-m} - 1), A^2(A - B)^2]^{\frac{1}{2}}. \quad (\text{B.12})$$

which represents the squared maximal Schmidt coefficient with respect to the bipartition  $P|Q$ , being  $P$  composed of  $m$  qubits.

By deriving the above expression as a function of  $m$ , it is not difficult to show that the bipartition that maximizes  $\lambda_{max}$  is the one with  $m = 1$ , i.e. a single qubit versus the rest, for any value of  $k$ . This finally provides the GME  $E_2$  of the state  $|\psi_{k,M=1}\rangle$ , in terms of the number  $n$  of qubits and the iteration step  $k$ .

Now we focus on states  $|\psi_{k,M=2}\rangle$  employed in the Grover search with two permutation invariant solutions. The reduced density matrix for the general bipartite splitting  $P|Q$ , where  $P$  ( $Q$ ) is composed of  $m$  ( $n - m$ ) qubits, is now

## B. Appendix

---

given by

$$\rho_P = \begin{pmatrix} c & b & \dots & b & d \\ b & a & \dots & a & b \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b & a & \dots & a & b \\ d & b & \dots & b & c \end{pmatrix}, \quad (\text{B.13})$$

where  $a, b, c$  are given below Eq. (B.9),  $d = a - 2A(A - B)$ , with now  $A = \cos \theta_k / \sqrt{2^n - 2}$  and  $B = \sin \theta_k / \sqrt{2}$ , and . Notice that we expect three non-vanishing eigenvalues, since the matrix  $\rho_P$  above has rank three.

We can reduce the diagonalization of  $\rho_P$  above to the diagonalization problem faced in the previous case with a single solution. We subtract the last column of  $\rho_P - \lambda \mathbb{1}$  from the first one and we substitute the first column for the obtained result. Then, we sum the first and the last row and divide the result by two. At last we substitute the last row for the previously found result, so that we are left with the following matrix

$$\begin{pmatrix} c - d - \lambda & b & \dots & b & d \\ 0 & a - \lambda & \dots & a & b \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & a & \dots & a - \lambda & b \\ 0 & b & \dots & b & \frac{1}{2}(c + d - \lambda) \end{pmatrix}. \quad (\text{B.14})$$

Therefore, it is straightforward to see that one eigenvalue is simply given by  $\lambda = c - d$  while the other two can be found following the procedure explained for the case of a single solution.

Once we know the non-vanishing eigenvalues of  $\rho_P$  in terms of  $m$ , we can maximize the largest one over all possible bipartitions  $m$ , eventually leading to the GME  $E_2$  of the state  $|\psi_{k,M=2}\rangle$  for two symmetric solutions. Notice that the above reasoning no longer works if we do not consider a permutation invariant state, since we can no longer focus only on the number  $m$  of qubits composing the bipartition  $P$ , but instead we have to specify the labels of the qubits we address case by case. This fact makes the calculation almost intractable.

# Appendix C

## C.1 Purity of the Choi state $C_{\mathcal{M}}$

An other interesting question concerns the purity of the state  $C_{\mathcal{M}} = (\mathcal{M} \otimes \mathcal{I})[|\alpha\rangle\langle\alpha|]$  corresponding to the CP-TP map  $\mathcal{M}$  via the Choi-Jamiołkowski isomorphism. Under which assumptions is the state  $C_{\mathcal{M}}$  pure?

We show here that the state  $C_{\mathcal{M}}$  is pure if and only if the map  $\mathcal{M}$  acting on  $\mathcal{D}(\mathcal{H})$  has a single Kraus operator. It is clear that one direction is trivial: if the map has a single Kraus operator  $A$  then, the corresponding Choi state  $C_{\mathcal{M}} = (A \otimes \mathbb{1})|\alpha\rangle\langle\alpha|(A^\dagger \otimes \mathbb{1})$  is pure by construction. But, what about the inverse?

In order to answer this question, let us consider first the case in which the given map  $\mathcal{M}$  has two Kraus operators  $\{A, B\}$ , fulfilling the constraint

$$A^\dagger A + B^\dagger B = \mathbb{1}, \quad (\text{C.1})$$

coming from the TP property. By tracing out both sides, it follows that

$$\|A\|^2 + \|B\|^2 = d \quad (\text{C.2})$$

being  $d$  the dimension of the Hilbert space  $\mathcal{H}$ , and where we have introduced the Hilbert-Schmidt norm of an operator  $X$  as

$$\|X\| = \sqrt{\text{Tr}[X^\dagger X]}. \quad (\text{C.3})$$

The bipartite state corresponding to the map  $\mathcal{M}$  is then given by

$$C_{\mathcal{M}} = (A \otimes \mathbb{1})|\alpha\rangle\langle\alpha|(A^\dagger \otimes \mathbb{1}) + (B \otimes \mathbb{1})|\alpha\rangle\langle\alpha|(B^\dagger \otimes \mathbb{1}). \quad (\text{C.4})$$

Therefore, imposing the purity condition  $\text{Tr}[C_{\mathcal{M}}^2] = 1$ , we get

$$\|A\|^4 + \|B\|^4 + 2|\text{Tr}[A^\dagger B]|^2 = d^2, \quad (\text{C.5})$$

thanks to the identity  $\langle\alpha|(A^\dagger B \otimes \mathbb{1})|\alpha\rangle = \frac{1}{d}\text{Tr}[A^\dagger B]$ . Since the constraint given by Eq. (C.2) always holds for a TP map, we can merge that condition with the purity one, arriving at

$$|\text{Tr}[A^\dagger B]|^2 = \|A\|^2\|B\|^2. \quad (\text{C.6})$$



A way to argue that  $A$  and  $B$  must be the same operator is the following. We recall the Cauchy-Schwartz inequality for the space of operators, namely

$$|\text{Tr}[A^\dagger B]| \leq \|A\| \|B\|, \quad (\text{C.7})$$

and remind that the equality holds if and only if the two operators are the same. Therefore, looking at Eq. (C.6), it is straightforward to see that the purity condition holds if and only if we have a single Kraus operator. Notice that the case with more than two Kraus operators can be treated in the same way, applying at the end a proof by contradiction.

This note definitely concludes the proof, so the Choi state  $C_{\mathcal{M}}$  corresponding to a given CP-TP map  $\mathcal{M}$  is pure if and only if the map  $\mathcal{M}$  has a single Kraus operator  $A$  fulfilling  $A^\dagger A = \mathbb{1}$ . Notice that if the dimension of the Hilbert space is finite then  $A$  is unitary too, since  $A^\dagger A = \mathbb{1}$  implies  $AA^\dagger = \mathbb{1}$  for finite dimension  $d$ .

## C.2 Schmidt decomposition of $Z_3$ and calculation of $\alpha_{SRU}$

Consider the gate  $Z_3$  defined as  $Z_3 = \text{diag}(1, 1, 1, 1, 1, 1, 1, 1, -1)$  and acting on two qutrits, i.e. two systems of dimension  $d = 3$ . The above gate is clearly unitary and not separable. By the help of the local basis composed of the nine elements

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \dots, E_9 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (\text{C.8})$$

we can express  $Z_3$  as  $Z_3 = \sum_{i,j=1}^9 C_{ij} E_i \otimes E_j$  with  $C_{ij} = \text{Tr}[(E_i^\dagger \otimes E_j^\dagger) Z_3]$ . Then, by performing the singular value decomposition [1] of the matrix  $C$  of coefficients, we can rewrite  $Z_3$  in the Schmidt form, with Schmidt rank  $r = 2$ , as

$$Z_3 = \lambda_1 A_1 \otimes B_1 + \lambda_2 A_2 \otimes B_2, \quad (\text{C.9})$$

where  $\lambda_{1,2} = \sqrt{\frac{1}{2}(9 \pm \sqrt{17})}/3$  and

$$A_{1,2} = \frac{\sqrt{3}}{\sqrt{102 \pm 22\sqrt{17}}} [(5 \pm \sqrt{17})(E_1 + E_5) + (1 \pm \sqrt{17})E_9], \quad (\text{C.10})$$

$$B_{1,2} = \frac{\sqrt{3}}{\sqrt{646 \pm 150\sqrt{17}}} [(11 \pm 3\sqrt{17})(E_1 + E_5) + (9 \pm \sqrt{17})E_9]. \quad (\text{C.11})$$

Notice that, despite ugly numbers, the four operators  $A_{1,2}$  and  $B_{1,2}$  have a very convenient diagonal matrix representation given by

$$A_{1,2} = \frac{\sqrt{3}}{\sqrt{102 \pm 22\sqrt{17}}} \text{diag}(5 \pm \sqrt{17}, 5 \pm \sqrt{17}, 1 \pm \sqrt{17}), \quad (\text{C.12})$$

$$B_{1,2} = \frac{\sqrt{3}}{\sqrt{646 \pm 150\sqrt{17}}} \text{diag}(11 \pm 3\sqrt{17}, 11 \pm 3\sqrt{17}, 9 \pm \sqrt{17}), \quad (\text{C.13})$$

which are clearly not unitary operators. This makes clear that the value of the maximum overlap  $\alpha_S$  is  $\alpha_S = \lambda_1 = \sqrt{\frac{1}{2}(9 + \sqrt{17})}/3 \simeq 0.854$ . Now we may wonder whether there exists a separable unitary  $U_A \otimes U_B$  such that achieves this maximum value as well. In the following we will prove that this is not the case.

In order to show that two local unitaries  $U_A, U_B$  achieving such a maximum overlap do not exist, let us decompose the general  $U_A$  and  $U_B$  as

$$U_A = \sum_{i=1}^{d^2} \alpha_i A_i, \quad U_B = \sum_{i=1}^{d^2} \beta_i B_i, \quad (\text{C.14})$$

where  $\{\alpha_i\}_{i=1,\dots,d^2}, \{\beta_i\}_{i=1,\dots,d^2}$  are complex coefficients, and  $\{A_i\}, \{B_i\}$  represent the bases coming from the Schmidt decomposition of  $Z_3$ . Recall that the first two operators  $A_{1,2}$  and  $B_{1,2}$  are given by Eqs. (C.12), (C.13), respectively. We can then calculate the maximum overlap

$$\alpha_{SRU} = \frac{1}{d^2} \max_{U_A, U_B} |\text{Tr}[(U_A^\dagger \otimes U_B^\dagger)U]|, \quad (\text{C.15})$$

by numerically maximizing over the complex parameters  $\{\alpha_i\}, \{\beta_i\}$ , fulfilling the unitary constraints  $U_A^\dagger U_A = \mathbb{1}$  and  $U_B^\dagger U_B = \mathbb{1}$ . This eventually leads to  $\alpha_{SRU} \simeq 0.786$ .

As a side result we mention that, in order to achieve  $\alpha_{SRU} \simeq 0.786$  as the overlap between  $Z_3$  and local unitaries, it is not restrictive here to consider only the first two terms composing  $U_A$  and  $U_B$ , i.e.

$$U_A = \alpha_1 A_1 + \alpha_2 A_2, \quad U_B = \beta_1 B_1 + \beta_2 B_2. \quad (\text{C.16})$$

In fact, besides the Schmidt decomposition of  $Z_3$  involves only the two terms  $A_1 \otimes B_1$  and  $A_2 \otimes B_2$  (thus, they are the only ones contributing to the overlap  $\alpha_{SRU}$  of (C.15)), the unitary constraints might in general not allow for the simple decomposition (C.16). In other words, a decomposition of  $U_A$  and  $U_B$  in terms of more components  $\{A_i\}$  and  $\{B_i\}$ , respectively, might weaken the unitary constraints, resulting in a larger overlap  $\alpha_{SRU}$ . We nevertheless believe that, even with unitary constraints, considering more components of  $U_A$  and  $U_B$  would never improve the overlap  $\alpha_{SRU}$  found with the minimal number of terms. However, up to now our statement has not been proved, and the question remains open.



# Appendix D

## D.1 QCD experimental set-up

**SPDC source:** The two-photon source used in this experiment is depicted in Fig. D.1: a type I,  $0.5\text{ mm}$ -long BBO crystal, illuminated back and forth by a CW laser at  $355\text{ nm}$  generates two H-polarized cones of photon pairs by spontaneous parametric down-conversion (SPDC). One of the cones is transformed into a V-polarized cone by the combined action of a spherical mirror and a quarter-wave plate, thus allowing the production of polarization-entangled photon pairs, on two spatial modes selected by a 2-hole mask (Fig. D.1 (a), [78]). Four spatial modes of emitted pairs ( $r_A$ - $l_B$  and  $l_A$ - $r_B$ ) can be selected by use of a 4-hole mask instead, thus allowing the generation of path-polarization hyper-entangled photon pairs (Fig. D.1 (b), [79]).

**Depolarizing channel:** The 1-qubit depolarizing channel acting on Bob's photon consists of two liquid crystal retarders ( $\text{LC}_1$  and  $\text{LC}_2$ ), the fast axis of  $\text{LC}_1$  being horizontal and the one of  $\text{LC}_2$  being oriented at  $45^\circ$ . Thus,  $\text{LC}_1$  acts as  $\mathbb{1}$  or  $\sigma_z$  when the applied voltage is  $\mathcal{V}_1$  or  $\mathcal{V}_\pi$  respectively,  $\text{LC}_2$  acts as  $\mathbb{1}$  or  $\sigma_x$  when the applied voltage is  $\mathcal{V}_1$  or  $\mathcal{V}_\pi$  respectively, and they act as  $\sigma_y$  when  $\mathcal{V}_\pi$  is applied to both. The weight  $p$  is varied by changing the duration

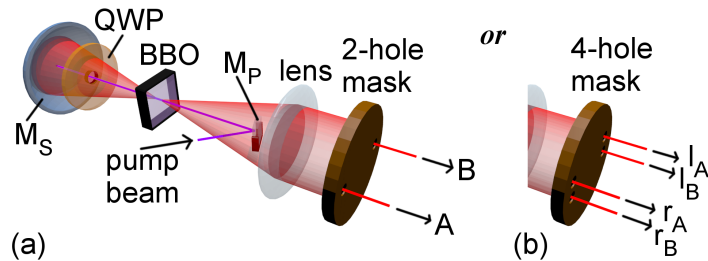


Figure D.1: Sketch of the SPDC source of two-photon polarization entangled states (a) or path-polarization hyper-entangled states (b). BBO:  $\beta$ -barium borate crystal,  $M_P$ : pump mirror,  $M_S$ : spherical mirror, QWP: quarter-wave plate.

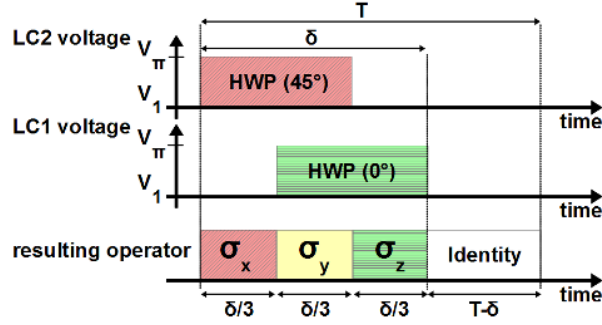


Figure D.2: Implemented Pauli operators during a detection gate.  $\delta$ : time when  $\mathcal{V}_\pi$  is applied to  $\text{LC}_1$  and/or  $\text{LC}_2$ ,  $T$ : detection gate duration; during  $T - \delta$ ,  $\mathcal{V}_1$  is applied to both  $\text{LC}_1$  and  $\text{LC}_2$ .

$\delta$  of the voltage  $\mathcal{V}_\pi$  on each LC with respect to the detection gate duration  $T$ :  $p = \frac{\delta}{T}$  (Fig. D.2, [76]).

**Two-qubit CNOT gate:** The detailed experimental set-up of the 2-qubit separable map detection is shown in Fig. D.3.  $\text{LC}_1$  ( $\text{LC}_2$ ) and  $\text{glass}_1$  ( $\text{glass}_2$ ) implement a 2-qubit dephasing process on photon  $B$  before (after) the CNOT gate; the path qubits are analysed with a beam-splitter (BS) and two glass plates ( $\phi_A$  and  $\phi_B$ ) with a delay  $\Delta x = 0$  between the left and the right path; a half-wave plate (HWP) and a polarizing beam-splitter (PBS) are used to analyse the polarization qubits; the photons are detected in coincidence by two fibered single-photon avalanche photodiodes (SPAD).

Note that the Pauli operators for the polarization qubits  $1, 3$  can be expressed as:  $\sigma_x^{(i)} = |D\rangle_i\langle D|_i - |A\rangle_i\langle A|_i$ ,  $\sigma_y^{(i)} = |L\rangle_i\langle L|_i - |R\rangle_i\langle R|_i$ ,  $\sigma_z^{(i)} = |H\rangle_i\langle H|_i - |V\rangle_i\langle V|_i$ , where  $D$ ,  $A$ ,  $L$  and  $R$  design the linear diagonal, linear anti-diagonal, circular left and circular right polarization, respectively, and  $i = A, B$ . For the path qubits  $2, 4$ , the Pauli operators can be written as:  $\sigma_x^{(i)} = |d\rangle_i\langle d|_i - |a\rangle_i\langle a|_i$  and  $\sigma_z^{(i)} = |r\rangle_i\langle r|_i - |l\rangle_i\langle l|_i$ , where  $|d\rangle_i = \frac{1}{\sqrt{2}}(|r\rangle_i + |l\rangle_i)$  and  $|a\rangle_i = \frac{1}{\sqrt{2}}(|r\rangle_i - |l\rangle_i)$  are the diagonal and anti-diagonal path states, and  $i = A, B$ .

## D.2 Two-qubit CNOT gate: noise model

In order to model the imperfection of the experimental CNOT Choi state, we mainly consider two decoherence sources. Firstly, there is a depolarising process on the polarization degree of freedom given by the non perfect emission of the state  $|\Phi^+\rangle_{13}$  from the source. The noisy initial state can then be modelled as

$$\rho_{in} = (\nu_\pi |\Phi^+\rangle_{13} \langle \Phi^+| + (1 - \nu_\pi) \frac{\mathbb{1}_{13}}{4}) \otimes |\Psi^+\rangle_{24} \langle \Psi^+|, \quad (\text{D.1})$$

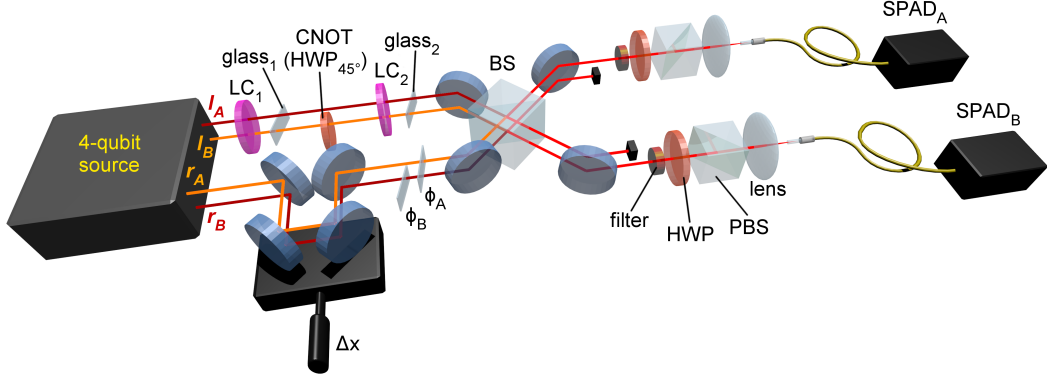


Figure D.3: Experimental set-up of the 2-qubit noisy CNOT channel. 4-qubit source: polarization-path hyperentangled two-photon source (Fig. D.1 (b)); CNOT: half-wave plate set at  $45^\circ$ ;  $LC_{1,2}$ : liquid crystal retarders set at  $0^\circ$ ;  $glass_{1,2}$ : thin glass plates; BS: 50-50 beam-splitter;  $\phi_A, B$ : thin glass plates;  $\Delta x$ : adjustable delay between the left and the right path; HWP: half-wave plate; PBS: polarizing beam-splitter; SPAD: fibered single-photon avalanche photodiodes.

where  $\nu_\pi$  is the visibility in the polarization degree of freedom, and  $|\Psi^+\rangle_{24}$  represents the noiseless initial state in the path degree of freedom. The polarization visibility can be measured experimentally leading to  $\nu_\pi = 0.858 \pm 0.008$ .

The second source of noise instead affects the path degree of freedom just before the measurement and models the non perfect superposition of modes at the BS level. The net experimental effect is a non perfect interference that can be theoretically described by the following dephasing channel  $\mathcal{D}_{BS}$ :

$$\rho \rightarrow (1 - \eta_k)^2 \rho + \eta_k(1 - \eta_k)[\sigma_z^{(2)} \rho \sigma_z^{(2)} + \sigma_z^{(4)} \rho \sigma_z^{(4)}] + \eta_k^2 \sigma_z^{(2)} \sigma_z^{(4)} \rho \sigma_z^{(2)} \sigma_z^{(4)}, \quad (D.2)$$

where the parameter  $\eta_k$  represents the strength of the dephasing process and can be connected to the path visibility  $\nu_k$  via the formula  $\nu_k = (1 - 2\eta_k)^2$  [77]. A path visibility  $\nu_k = 0.904 \pm 0.004$  is measured, hence an experimental value of about  $\eta_k = 0.025$  is found.

Therefore, instead of the perfect Choi state  $C_{\mathcal{M}_{D,X}}$  with  $\mathcal{M}_{D,X} = (\mathcal{D}_2 \otimes \mathcal{D}_2)\text{CNOT}(\mathcal{D}_1 \otimes \mathcal{D}_1)$ , we experimentally implemented the following noisy four-qubit state

$$\rho_{out} = \mathcal{D}_{BS} \circ \mathcal{M}_{D,X}[\rho_{in}], \quad (D.3)$$

with respect to which we calculate the expectation value of the detection operator  $\hat{W}_{\text{CNOT}}$  as a function of  $q_1$ ,  $q_2$ ,  $\nu_\pi$  and  $\eta_k$ . We recall the reader that the two parameters  $q_1$  and  $q_2$  are controlled experimentally and can be changed in order to make the CNOT gate nosier, while  $\nu_\pi$  and  $\eta_k$  model the unavoidable noise present in the experimental set-up. In the case with  $q_1 = q_2 = q$ , i.e. when the controlled dephasing processes before and after the CNOT gate have

## D. Appendix

---

the same strength, the following expectation value of  $\tilde{W}_{\text{CNOT}}$  over the state  $\rho_{out}$  given by Eq. (D.3) can be found:

$$\begin{aligned} \text{Tr}[\tilde{W}_{\text{CNOT}}\rho_{out}] = 1 - 2\nu_\pi + 2[2q^3 + \eta_k(\eta_k - 1)(2q - 1)^3](1 + \nu_\pi) \\ - 2q^2(3 + 4\nu_\pi) + q(3 + 5\nu_\pi). \end{aligned} \quad (\text{D.4})$$

By setting the measured values of  $\nu_\pi$  and  $\eta_k$ , the above expression is exploited to fit the experimental data of  $\tilde{W}_{\text{CNOT}}$  in terms of  $q$  (see Sec. 4.3 for further details).

# Bibliography

- [1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
- [2] P. W. Shor in *Proceedings of the 35th IEEE Symposium on the Foundations of Computer Science* (1994), pp. 124-134; P. W. Shor, SIAM J. Comput. **26**(5), 1484-1509 (1997).
- [3] L. K. Grover, in *Proceeding of the 28th Annual Symposium on the Theory of Computing* (ACM Press, New York, 1996), pp. 212-219; L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
- [4] D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A **439**, 553 (1992).
- [5] E. Bernstein and U. Vazirani, in *Proceeding of the 25th Annual Symposium on the Theory of Computing* (ACM Press, New York, 1993), p. 11.
- [6] D. Simon, in *Proceedings of the 35th IEEE Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 116.
- [7] R. Jozsa and N. Linden, Proc. R. Soc. Lond. A **459**, 2011 (2003).
- [8] D. Bruß and C. Macchiavello, Phys. Rev. A **83**, 052313 (2011).
- [9] D. Bruß and C. Macchiavello, Phys. Rev. A **85**, 049906 (2012).
- [10] D. Gottesman, arXiv:quant-ph/9807006 (1998).
- [11] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
- [12] A. Datta, A. Shaji and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
- [13] M. Van den Nest, Phys. Rev. Lett. **110**, 060504 (2013).
- [14] N. Linden and S. Popescu, Phys. Rev. Lett. **87**, 047901 (2001).
- [15] R. Jozsa, arXiv:quant-ph/9707034 (1997).



## BIBLIOGRAPHY

---

- [16] M. Rossi, M. Huber, D. Bruß and C. Macchiavello, New J. Phys. **15**, 113022 (2013).
- [17] M. Rossi, D. Bruß and C. Macchiavello, accepted for publication in Phys. Script. (2013).
- [18] M. Rossi, D. Bruß and C. Macchiavello, Phys. Rev. A **87**, 022331 (2013).
- [19] K. Kraus, *States, effects and operations* (Springer, Berlin, 1983).
- [20] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A **223**, 1 (1996); B. M. Terhal, Phys. Lett. A **271**, 319 (2000).
- [21] O. Gühne and G. Tóth, Phys. Rep. **474**, 1-75 (2009).
- [22] C. Macchiavello and M. Rossi, Phys. Rev. A **88**, 042335 (2013).
- [23] C. Macchiavello and M. Rossi, J. Phys.: Conf. Ser. **470**, 012005 (2013).
- [24] M. Horodecki, P. W. Shor and M. B. Ruskai, Rev. Math. Phys. **15**, 629 (2003).
- [25] J. I. Cirac, W. Dür, B. Kraus and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
- [26] E. M. Rains, arXiv:quant-ph/9707002 (1998).
- [27] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, Rev. Mod. Phys. **81**(2), 865 (2009).
- [28] C. Macchiavello and M. Rossi, Phys. Script. T**153**, 014044 (2013).
- [29] A. Orioux, L. Sansoni, M. Persechino, P. Mataloni, M. Rossi and C. Macchiavello, Phys. Rev. Lett. **111**, 220501 (2013).
- [30] G. M. D’Ariano, C. Macchiavello and M. Rossi, Phys. Rev. A **87**, 032337 (2013).
- [31] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
- [32] P. Arrighi, V. Nesme and R. F. Werner, Lecture Notes in Computer Science **5196**, 64-75 (2008).
- [33] P. Arrighi, V. Nesme and R. F. Werner, arXiv:0711.3975 (2009).
- [34] C. Kruszynska and B. Kraus, Phys. Rev. A **79**, 052304 (2009).
- [35] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest and H. J. Briegel, in *Proceedings of the International School of Physics “Enrico Fermi” on “Quantum Computers, Algorithms and Chaos”* (Varenna, Italy, 2005). Also available at arXiv:quant-ph/0602096.

- [36] T.-C. Wei and P. M. Goldbart, Phys. Rev. A **68**, 042307 (2003).
- [37] G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).
- [38] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
- [39] D. Gottesman, arXiv:quant-ph/9705052 (1997).
- [40] D. Schlingemann and R.F. Werner, Phys. Rev. A **65**, 012308 (2002).
- [41] T. Carle, B. Kraus, W. Dür and J. I. de Vicente, Phys. Rev. A **87**, 012328 (2013).
- [42] M. Davis and H. Putnam, J. of the ACM **7(3)**, 201 (1960); D. Marx, in *Proceeding of the 42nd Annual Symposium on the Theory of Computing* (ACM Press, New York, 2010), pp. 735-744.
- [43] D. Aharonov, in *Annual Reviews of Computational Physics VI*, edited by D. Stauffer (World Scientific, Singapore, 1999).
- [44] M. Blasone, F. Dell'Anno, S. De Siena and F. Illuminati, Phys. Rev. A **77**, 062304 (2008).
- [45] R. Hübener, M. Kleinmann, T.-C. Wei, C. González-Guillén and O. Gühne, Phys. Rev. A **80**, 032324 (2009).
- [46] Y. Fang, D. Kaszlikowski, C. Chin, K. Tay, L.C. Kwek, C.H. Oh, Phys. Lett. A **345**, 265 (2005).
- [47] R. Orús and J. I. Latorre, Phys. Rev. A **69**, 052308 (2004).
- [48] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).
- [49] L. K. Grover, Phys. Rev. Lett. **95**, 150501 (2005); T. Tuli, L. K. Grover and A. Patel, Quant. Inf. Comput. **6**, 483 (2006).
- [50] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
- [51] Z. Diao, M. S. Zubairy, and G. Chen, Z. Naturforsch. **57a**, 701 (2002).
- [52] R. Jozsa, preprint arXiv:quant-ph/0603163 (2006).
- [53] I. L. Markov and Y. Shi, SIAM Journal on Computing, **38(3)**, 963-981 (2008).
- [54] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972); M.-D. Choi, Linear Algebr. Appl. **10**, 285 (1975).
- [55] J. de Pillis, Pacific J. Math. **23**, 129 (1967).

## BIBLIOGRAPHY

---

- [56] A. Acín, D. Bruß, M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **87**, 040401 (2001).
- [57] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera, Phys. Rev. A **66**, 062305 (2002).
- [58] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera, J. Mod. Opt. **50**, 1079 (2003).
- [59] A. De Pasquale and V. Giovannetti, Phys. Rev. A **86**, 052302 (2012).
- [60] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999).
- [61] M. Steiner, Phys. Rev. A **67**, 054305 (2003).
- [62] F. G. S. L. Brandão, Phys. Rev. A **72**, 022310 (2005).
- [63] K. M. R. Audenaert and S. Scheel, New J. Phys. **10**, 023011 (2008).
- [64] C. Macchiavello and G. M. Palma, Phys. Rev. A **65**, 050301(R) (2002).
- [65] O. Gühne and P. Hyllus, Int. J. Theor. Phys. **42**, 1001 (2003).
- [66] A. G. White, A. Gilchrist, G. J. Pryde, J. L. O'Brien, M. J. Bremner and N. K. Langford, J. Opt. Soc. B **24**, 172 (2007).
- [67] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
- [68] M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow and A. Hines, Phys. Rev. A **67**, 052301 (2003).
- [69] O. Gühne, C.-Y. Lu, W.-B. Gao, and J.-W. Pan, Phys. Rev. A **76**, 030305(R) (2007).
- [70] E. M. Rains, Phys. Rev. A **60**, 179 (1999).
- [71] A. S. Holevo, *Quantum Systems, Channels, Information* (De Gruyter, Berlin, 2012).
- [72] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [73] P. Horodecki and A. Ekert, Phys. Rev. Lett. **89**, 127902 (2002).
- [74] K. Życzkowski and I. Bengtsson, Open Syst. Inf. Dyn. **11**, 3 (2004).
- [75] S. Virmani, S. F. Huelga, and M. B. Plenio, Phys. Rev. A. **71**, 042328 (2005).

- 
- [76] A. Chiuri, V. Rosati, G. Vallone, S. Pádúa, H. Imai, S. Giacomini, C. Macchiavello and P. Mataloni, Phys. Rev. Lett. **107**, 253602 (2011).
- [77] A. Chiuri, G. Vallone, N. Bruno, C. Macchiavello, D. Bruß and P. Mataloni, Phys. Rev. Lett. **105**, 250501 (2010).
- [78] C. Cinelli, G. Di Nepi, F. De Martini, M. Barbieri and P. Mataloni, Phys. Rev. A **70**, 022321 (2004).
- [79] M. Barbieri, C. Cinelli, P. Mataloni and F. De Martini, Phys. Rev. A **72**, 052110 (2005).
- [80] M. Barbieri, F. De Martini, G. Di Nepi, P. Mataloni, G. M. D'Ariano and C. Macchiavello, Phys. Rev. Lett, **91**, 227901 (2003).
- [81] J. Kempe, Cont. Phys **44**, 307 (2003).
- [82] A. Schreiber, A. Gábris, P. P. Rohde, K. Laiho, M. Štefaňák, V. Potoček, C. Hamilton, I. Jex and C. Silberhorn, Science **336**, 55 (2012).
- [83] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi and R. Osellame, Phys. Rev. Lett. **108**, 010502 (2012).
- [84] G. M. D'Ariano, Phys. Lett. A **376**, 697 (2012).
- [85] A. Bisio, G. M. D'Ariano and A. Tosini, arXiv:1212.2839 (2012).
- [86] L. Hardy, in *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*, edited by H. Halvorson (Cambridge University Press, New York, 2011), pp. 409-442.
- [87] G. M. D'Ariano, in *Quantum Theory: Reconsideration of Foundations*, 5, edited by A. Y. Khrennikov, AIP Conf. Proc. No. 1232 (AIP, Melville, NY, 2010), p. 3. Also available at arXiv:1001.1088.
- [88] H. P. Yuen, Phys. Lett. A **113**, 405 (1986).
- [89] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
- [90] D. Bruß, M. Cinchetti, G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
- [91] G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **76**, 042306 (2003).
- [92] T. Durt, J. Fiurášek and N. J. Cerf, Phys. Rev. A **72**, 052322 (2005).
- [93] F. Buscemi, G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **71**, 042327 (2005).
- [94] G. E. Andrews, *The Theory of Partitions*, (Cambridge University Press, Cambridge, 1976).



# List of Publications

1. M. Rossi, D. Bruß and C. Macchiavello, Phys. Rev. A **87**, 022331 (2013).
2. G. M. D'Ariano, C. Macchiavello and M. Rossi, Phys. Rev. A **87**, 032337 (2013).
3. C. Macchiavello and M. Rossi, Phys. Rev. A **88**, 042335 (2013).
4. C. Macchiavello and M. Rossi, Phys. Script. T**153**, 014044 (2013).
5. C. Macchiavello and M. Rossi, J. Phys.: Conf. Ser. **470**, 012005 (2013).
6. M. Rossi, D. Bruß and C. Macchiavello, accepted for publication in Phys. Script. (2013).
7. M. Rossi, M. Huber, D. Bruß and C. Macchiavello, New J. Phys. **15**, 113022 (2013).
8. A. Orioux, L. Sansoni, M. Persechino, P. Mataloni, M. Rossi and C. Macchiavello, Phys. Rev. Lett. **111**, 220501 (2013).

